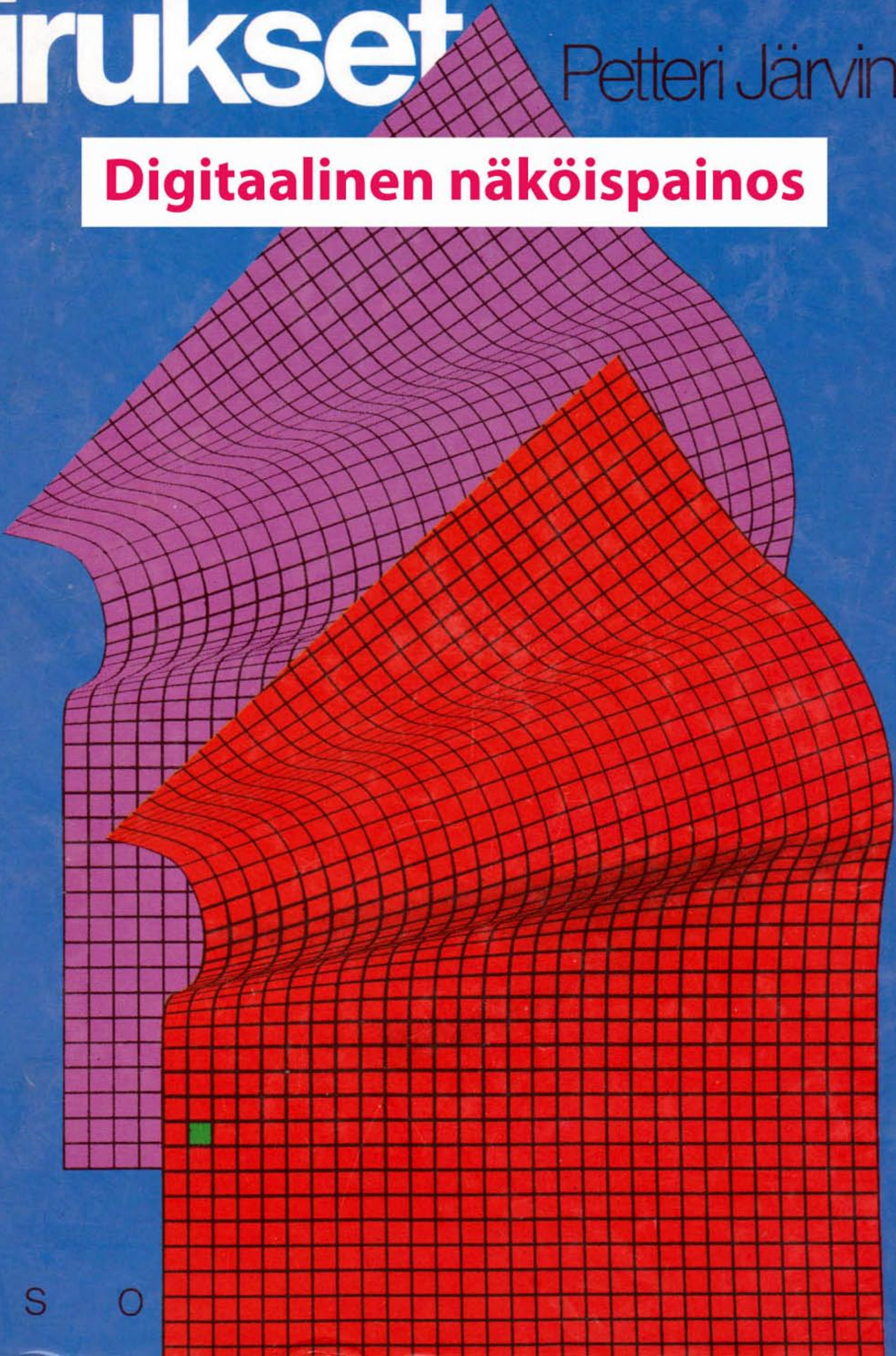
tietokone-virukset

Petteri Järvinen

Digitaalinen näköispainos



W S O Y

Saate digitaaliseen näköispainokseen

Kun kirja Tietokonevirukset ilmestyi syksyllä 1990, se oli edellä aikaansa. Viruksista puhuttiin kyllä mediassa, mutta todellista vaaraa niistä ei vielä ollut. Pääasiallinen leviämistapa oli levykkeiden välityksellä: käyttäjä unohti vieraan lerpun (=levykkeen) asemaan ja käynnisti koneen sillä, jolloin levykkeen käynnistyslohkossa piileskellyt haittakoodi pääsi muistiin ja levitti itseään uusiin levykkeisiin.

Oli myös tiedostoviruksia, jotka tarttuivat ohjelmien perään ja levisivät uusiin ohjelmiin niiden käynnistyksen yhteydessä. Ei ollut sähköpostia, tietoliikennettä eikä internetiä, joten omalla huolellisuudella viruksilta oli mahdollista välttyä.

Todistaakseni, että viruksista varoittelu ylipäätään oli aiheellista, kuljetin mukanani punaista levykelaatikkoa, johon oli isolla mustalla tussilla kirjoitettu varoitus viruksista. Sain ilmoituksia käyttäjiltä ja kiersin keräämässä heidän koneistaan näytteitä. Osa lähetti epäilyttäviä levykkeitä postissa. Niitä on vieläkin tallella iso pahvilaatikollinen.

Viruspelot konkretisoituivat pari vuotta myöhemmin. Maaliskuussa 1992 levinnyt Michelangelo oli ensimmäisiä laajoja pc-epidemioita. Kokonaan uusi vaihe alkoi 90-luvun lopulla, kun dokumenttivirukset levisivät Word-tiedostojen ja sähköpostin mukana (Melissa, I Love You ym). Seuraavan vuosituhannen alku oli liki painajaismaista aikaa, kunnes käyttöjärjestelmien ja sovellusten turva-aukot saatiin korjattua ja palomuurit yleistyivät.

Virusten hiipuessa tilalle tulivat nettirikolliset, kiristysohjelmat, monenmoiset nettihuijaukset ja valtiolliset vakoiluohjelmat. Mutta ne ovat jo muiden kirjojen aiheita.

Julkaisen kirjan vapaasti jaettavana pdf-versiona, jotta jälkipolville jäisi ajankuva tietokonevirusten alkuhämäristä ja käsitys tietoturvan kehittymistä.

Espoossa syyskuussa 2020,

Petteri Järvinen

Sisällys

Esipuhe

Tämä kirja kertoo kokonaan uudesta teknisen aikakauden ilmiöstä: tietokoneviruksista. Kyse on tietokoneohjelmista, jotka on ohjelmoitu käyttäytymään luonnollisten virusten tapaan. Ne lisääntyvät, leviävät tietokoneesta toiseen ja tuottavat harmia niin mikroille kuin niiden käyttäjillekin.

Sitä mukaa kun tunnettujen tietokonevirusten määrä on maailmalla kasvanut, ovat myös tiedotusvälineet alkaneet kiinnittää huomiota asiaan. Viruksista levitetty tieto on usein ollut epätarkkaa, joko viruksia vähättelevää tai niillä pelottelevaa. Tietoja levittävät henkilöt eivät läheskään aina ole ymmärtäneet tietokonevirusten olemusta ja toimintamekanismeja. Monet heistä eivät itse ole edes nähneet yhtään tietokonevirusta. Tämän valossa on helppo ymmärtää, miksi tietokoneviruksiin liittyy niin monia virheellisiä uskomuksia.

Ennen virusten torjunta oli helppoa. Riitti, kun vältti kavereilta kopioituja pelejä ja käytti vain kaupasta ostettuja ohjelmia. Kun viruksia alkoi löytyä myös kaupasta ostetuista ohjelmista huomattiin, ettei kukaan ollut täysin turvassa näiltä kiusankappaleilta. Ne saattoivat tarttua kenen mikroon tahansa ja aiheuttaa huomattavia vahinkoja.

Tänä päivänä virukset muodostavat uhkan, joka kaikkien mikronkäyttäjien on otettava huomioon. ATK-päälliköiden, mikrotukihenkilöiden, koulujen atk-opettajien ja muiden vastaavien pitäisi tietää, mitä virukset ovat, miten ne leviävät, mitä ne voivat tehdä ja miten niitä torjutaan.

Tämän kirjan tarkoituksena on jakaa asiallista ja käyttökelpoista tietoutta tietokoneviruksista. Siinä on omat vaaransa. Tieto on valtaa ja tietoa voidaan käyttää monella eri tavalla. Kun talonmies kiinnittää talon seinään kilven "Läpikulku kielletty", hän haluaa estää ihmisiä kulkemasta pihan poikki. Tahtomattaan kilpi kertoo myös sen, että läpikulku ylipäätänsä on mahdollista. Kilpi toimii sekä tarkoituksensa puolesta että sitä vastaan.

Jo pelkkä viruksista kertominen on vaarallista. Viruksille annettu maailmanlaajuinen huomio luo "terroristiefektin", joka saa tällaisesta julkisuudesta kiinnostuneet henkilöt tuottamaan yhä uusia viruksia. Mistäpä tekijä muuten tietäisi, miten hänen viruksensa on maailmalla levinnyt, ellei hän voisi lukea siitä lehdistä.

Onneksi meillä Suomessa tilanne on toinen. Meiltä tuskin löytyy ketään, joka olisi todella tehnyt viruksia tai edes monta, jotka siihen pystyisivät. Osa mikrojen käyttäjistä nukkuu kuitenkin Ruususen unta Prinsessan tavoin tietämättä lainkaan niistä vaaroista, joita tietokoneviruksiin liittyy. He tarvitsevat tietoa. Tieto auttaa varautumaan siten, että viruksen tarttuminen omaan koneeseen tulee mahdollisimman vaikeaksi. Tieto neuvoo käyttäjälle merkit, joita tarkkailemalla virustartunnan voi havaita mahdollisimman aikaisin, jolloin sen taltuttaminen on vielä helppoa. Tieto mahdollistaa toipumisen mahdollisen viruksen aiheuttamista vahingoista. Tieto auttaa myös käyttäjiä voittamaan pelkonsa kun se osoittaa, että vain pieni osa kaikista tietokoneviruksista on suoranaisesti vahingollisia. Tämä kirja pyrkii jakamaan juuri tällaista tietoa.

Silti tiedossani on monia, lähinnä tekniikkaan liittyviä asioita, joita en ole voinut kirjassa kertoa. Niiden julkistaminen helpottaisi virusten tekemistä ja saattaisi houkutella suomalaisiakin kunnostautumaan tällä kyseenalaisen kunnian alueella. Vaikka virusten ohjelmointi vaatiikin huomattavaa asiantuntemusta, on mahdollista käyttää eräitä työtä helpottavia oikopolkuja. Niistä tämä kirja ei kerro.

Vaihtoehto tiedon jakamiselle on sen pimittäminen ja asioista vaikeneminen. Pahinta kai olisi, jos tietokonevirukset saisivat vapaasti levitä koneesta toiseen kenenkään nostamatta meteliä asiasta. Tiedon puuttuessa liikkeelle lähtisivät huhut, jotka vain entisestään pahentaisivat asiaa. Tietoa siis tarvitaan, mutta sen on oltava asiallista.

Hyötykäyttöön tarkoitetuista mikroista noin 85% on ns. PC-koneita, jolloin niiden käyttöjärjestelmänä on joko DOS, OS/2 tai Windows. Tämä näkyy myös kirjan painotuksessa, sillä suurin osa käsitellyistä viruksista liittyy juuri PC-koneisiin. Virusten toimintaan ja torjuntaan liittyvät tiedot ovat kuitenkin yleispäteviä ja sopivat kaikkiin tietoko-

neisiin - olipa kone sitten pieni kotimikro, iso supertietokone tai jotain tältä väliltä. Kaikissa koneissa kulkevat samanlaiset sähkövirrat.

Tällä kirjalla on kaksi erilaista käyttötarkoitusta. Toisaalta kirjan voi lukea mielenkiintoisena teknisenä seikkailuna jolloin on saa havaita, miten ihmisen oma elämä peilautuu hänen luomuksissaan. Ihminen on tehnyt koneet omiksi kuvikseen. Toisaalta kirja toimii virustorjunnan käsikirjana joka kannattaa kaivaa esille viimeistään silloin, kun omasta tietokoneesta löytyy virus ja halutaan tietää, miten kyseinen virus toimii ja miten siitä parhaiten pääsee eroon.

Ovatko virukset sitten todellinen uhka tietokoneiden käyttäjille? Kyllä ja ei. Teoriassa virukset pystyvät aiheuttamaan suurta vahinkoa ja merkittäviä taloudellisia seuraumuksia. Pahinta on, että tietokonevirusten lisääntyy huolestuttavan nopeasti. Joka kuukausi löydetään maailmalla useita uusia, ennestään tuntemattomia viruksia. Lisäksi viruksiin liittyy suorastaan pelottavia mahdollisuuksia sabotaasin ja sodankäynnin alueilla. Tänään ne ovat vasta mielenkiintoisia ajatusleikkejä, mutta eräät niistä saattavat konkretisoitua jo lähitulevaisuudessa.

Vielä ei onneksi olla niin pitkällä. Vaikka tietokonevirukset ovat Suomessakin aiheuttaneet vahinkoa, on monin verroin enemmän tietoa menetetty perinteisten laitevikojen ja käyttäjien omien virheiden vuoksi. Tiedotusvälineet ovat antaneet viruksille kohtuuttomankin paljon huomiota niiden aiheuttaman uhkan huomioon ottaen. Asiat pitäisi aina nähdä oikeissa mittasuhteissa. Churchillin kansalaisilleen antama ohje toisen maailmansodan sytyttyä pätee yhä: *Ainoa, mitä meidän tulee pelätä, on pelko itse.*

Toivottavasti tilanne myös säilyy tällaisena. Paljon riippuu siitä, miten hyvin käyttäjät oppivat varautumaan viruksiin ja miten pian uudet virukset saadaan kiinni. Uskon, että kirjani pystyy tätä kautta vaikuttamaan asioihin myönteisesti.

Lukijoissa saattaa olla sellaisia, joita kiinnostaa kirjan tekninen toteutus. Heitä varten muutama sana kirjan vaiheista. Koko kirja tehtiin Windows-ympäristössä. Teksti kirjoitettiin Word for Windowsilla ja lopullinen taittaminen sekä kuvien yhdistäminen tehtiin Ami Professio-

nalilla. DOS-ohjelmien kuvat on otettu ruudulta Hijaak-ohjelman avulla, muutettu PCX-muotoon ja tarvittaessa korjailtu Windowsin Paintbrushilla ennen siirtämistä tekstiin. WSOYlle kirja toimitettiin painovalmiina PostScript-kielisenä ohjelmana kahdella 3,5" korpulla.

Lopuksi haluan kiittää kaikkia niitä, jotka ovat vaikuttaneet tämän kirjan syntyyn lähettämällä tutkittavakseni niin aitoja kuin vaarattomiksikin osoittautuneita virusnäytteitä. Ilmoituksia havaituista tai epäillyistä viruksista voi jatkossakin lähettää tekijälle sähköpostin välityksellä (ELISA-tunnus Järvinen Petteri) tai Tietokone-lehden toimituksen kautta (Tietokone, Petteri Järvinen, PL 64, 00381 HELSINKI).

Tapiolassa 18.3.- 30.7.90

Petteri Järvinen

1

Virukset, madot ja muut tuholaiset

Yleisessä kielenkäytössä termi "virus" on vakiintunut tarkoittamaan melkein mitä tahansa ohjelmaa, joka tuottaa harmia pahaa-aavistamattomalle käyttäjälle. Virukset muodostavat kuitenkin vain pienen osan erilaisista vahingollisista ohjelmista. Vahingon takana voi yhtä hyvin olla viaton ohjelmointivirhe tai Troijan hevonen. Ennen kuin aletaan tarkastella varsinaisia viruksia, onkin paikallaan esitellä lyhyesti myös muita tuholaisia.

Ohjelmointivirheet

Ohjelmoijatkin ovat vain ihmisiä. Vaikka he yrittävät parhaansa - valvovat yömyöhään ohjelmansa kimpussa, pilaavat terveytensä kahvilla tai tupakalla ja testaavat ohjelmaansa toimitushetkeen asti - jää ohjelmiin silti joskus virheitä. Useimmiten virheet ovat pieniä eivätkä haittaa ohjelman käyttöä. Vain harvoin virheistä aiheutuu käyttäjälle suoranaista vahinkoa. Tällaisten tilanteiden varalta useimpien ohjelmien käsikirjoista tai lisenssiehdoista löytyy lause, jolla tekijä sanoutuu irti kaikesta vastuusta. Varsinkin USAssa lause on tarpeen, sillä lakimiehet ja -naiset suorastaan herkuttelevat miljooniin dollareihin nousevilla korvausvaatimuksilla.

Useinkaan virheen syy ei johdu suoranaisesti ohjelmoijasta. Tekninen kehitys on tuonut markkinoille niin monta erilaista järjestelmää,

ettei ohjelmoija millään voi testata konettaan kaikilla eri kokoonpanoilla. Lisäksi uusia laajennuksia ja oheislaitteita julkistetaan koko ajan. Ongelmia voi syntyä, kun hienoja uusia järjestelmiä käytetään vanhoilla ohjelmilla.

Ennen tilanne oli helpompi. Ehdoton markkinajohtaja oli IBM ja kun ohjelmoija testasi työnsä toimivuuden IBM PC:ssä, se riitti. Mikäli käyttäjällä oli jokin muu kuin IBM-mikro, se oli hänen ongelmansa. Sittemmin IBM on kuitenkin menettänyt ehdottoman markkinajohtajan aseman ja monet muut isot valmistajat ovat alkaneet tehdä hieman IBM:n mikroista poikkeavia koneita. Markkinoiden laajeneminen on tiennyt uusien yhteensopivuusongelmien syntymistä.

Laitesuunnittelijat ovat ihmisiä ja hekin tekevät virheitä. Esimerkiksi Intelin levykeaseman ohjaukseen käytetystä Intelin 8272A-mikropiiristä löytyi suunnitteluvirhe, joka eräissä harvoissa tapauksissa saattoi aiheuttaa virheellisiä kirjoitusoperaatioita levykkeelle. Vika havaittiin vasta kun piiriä oli ehditty käyttää jo noin 25 miljoonassa mikrossa!

Omalle kohdalleni on osunut parikin tapausta, jossa ohjelmavirheiden tai yhteensopivuuden puuttumisen vuoksi ohjelma on aiheuttanut vahinkoa. Toinen tapauksista liittyi PC-Toolsin 4-version mukana tulleeseen PC-Cache -ohjelmaan. Se sotki kiintolevyni E: aseman kirjanpidon aina kun yritin käyttää sitä.

Vielä huonommin kävi eräälle lääkärille, joka oli tekemässä väitöskirjaansa PC:llä. Laitetoimittaja oli asentanut koneeseen ison kiintolevyn ja vanhan DOS 3.2-version. Koska vasta DOS 3.3 tukee yli 32 megatavun levyjä, oli apuun haettu Disk Manager-niminen apuohjelma. Sillä levy oli jaettu osiin niin, että DOS 3.2 pystyi käyttämään levyä.

Lääkäri käynnisti koneessaan Nortonin Disk Doctorin, joka ei ilmeisestikään tuntenut Disk Managerin käyttämää tapaa kiintolevyn jakamiseen. Luullen levyn olevan täynnä virheitä Disk Doctor yritti korjata sen, jolloin tuloksena oli levyn täydellinen sekoaminen.

Madot

Termi mato (worm) tarkoittaa ohjelmaa, joka "kiemurtelee" koneen keskusmuistissa ja lisääntyy kopioimalla itseään kunnes keskusmuisti on tullut täyteen. Muistin täyttyminen pysäyttää yleensä koneen tai ainakin hidastaa sitä niin paljon, että koneen käyttäminen tulee mahdottomaksi.

Koska jokaisesta madosta syntyy oma prosessinsa, on madon luikertelu ja lisääntyminen mahdollista vain moniajoon pystyvässä koneessa. DOSissa tätä ominaisuutta ei ole. Siksi varsinaisia matoja voidaan tehdä vain isoissa tietokoneissa, Unix-koneissa tai mikrojen moniajoon pystyvissä käyttöjärjestelmissä (kuten OS/2).

Corewars

AT&T:n tutkimuslaboratorio on tullut kuuluisaksi monien siellä tehtyjen keksintöjen myötä. Eräs näistä keksinnöistä oli Corewars-niminen peli (suomeksi suunnilleen "keskusmuistisodat"), jossa kaksi ohjelmoijaa pelasi toisiaan vastaan. Molemmat kirjoittivat pienen ohjelman, joka pyrki luomaan itsestään mahdollisimman monta kopiota tietokoneen muistiin ja syömään toisen pelaajan matoja. Se, joka sai vallattua kaiken muistin itselleen ja tuhottua vastapuolen madot, oli voittaja. Tästä pelistä tuli kaikkien myöhempien mato-ohjelmien esikuva.

Corewars-peli oli pitkään salaisuus, jonka tunsivat vain asialleen omistautuneet ohjelmoijat. Pelistä haluttiin vaieta, koska useimmat pitivät sitä kalliin tietokoneajan tuhlauksena. Julkinen siitä tuli vasta vuonna 1983, kun Unixin kehittäjänä tunnettu Ken Thompson kertoi pelistä Turing-palkinnon jakotilaisuudessa. Kuvaus pelistä sekä ohjeet omien matojen tekemistä varten julkaistiin Scientific American -lehden toukokuun 1984 numerossa.

Mato Unix-verkossa

Viimeaikaisista madoista tunnetuin alkoi levitä marraskuun toisen päivän iltana 1988. Cornellin yliopistossa opiskellut 23-vuotias Robert Tappan Morris halusi kokeilla, toimivatko hänen Unixista löytämänsä turvallisuusaukot käytännössä. Hän kirjoitti aukkoja käyttävän ohjelman ja käynnisti sen koulunsa Unix-koneessa, joka oli muiden Unix-koneiden tavoin liitetty elektroniseen Internet-tietoverkkoon. Internet-verkko yhdistää toisiinsa lähes 200000 tietokonetta yliopistoissa, tutkimuskeskuksissa ja armeijan laitoksissa.

Mato lähti leviämään verkossa kulkevan elektronisen postin välityksellä. Kun vastaanottaja avasi saamansa postin, mato-ohjelma kävi tutkimassa hänen postituslistaansa ja lähetti itse itsensä kaikille listassa mainituille. Mato kuljetti mukanaan sanakirjaa, jossa oli lueteltu yleisiä salasanoja. Käyttäjätunnuksen ja listasta saatujen salasanojen avulla virus yritti päästä sisään uusiin koneisiin. Kun pääsy onnistui, mato-ohjelma alkoi tehdä monimutkaisia mutta hyödyttömiä laskutoimituksia, joiden tarkoituksena oli vain kuormittaa koneen prosessoria.

Morrisin tarkoituksena oli ollut ujuttaa yksi mato jokaiseen verkossa olevaan koneeseen ja pitää se siellä käynnissä kenenkään huomaamatta. Tämän varmistamiseksi matoon oli lisätty suojaus, joka ei kuitenkaan toiminut. Mato alkoi levitä myös yhden koneen sisällä ja 12 tunnin kuluttua useimmat madon saaneista 6000 koneesta olivat niin jumissa, että järjestelmät piti sulkea, käynnistää uudestaan ja puhdistaa. Unix-koneen sammuttaminen ja uusi käynnistäminen on työläs prosessi eikä siihen PC:n tapaan riitä pelkkä Ctrl-Alt-Delin painaminen.

Havaittuaan matokokeilun riistäytyneen käsistään Morris yritti lähettää verkkoon varoituksen madosta ja ohjeet sen nitistämiseksi. Koulun kone oli kuitenkin jo niin jumissa, ettei lähetys enää toiminut. Muiden koneiden operaattorit havaitsivat nopeasti, mitä oli tekeillä ja tieto madosta levisi verkon kautta kulovalkean tavoin. Koneita kytkettiin irti verkosta tartunnan estämiseksi. Verkon kautta madon saivat mm. Bostonin, Stanfordin, Harvardin ja Columbian yliopistot sekä San Franciscolainen Lawrence Livermore National Laboratory, joka on yksi ydinaseita suunnittelevista laboratorioista. Eräissä armeijan laitok-

```
Date:  Tuh, 3 Nov 88 06:46 EST
From: Stoll@DOCKMASTER.ARPA
Subject:  Virus on the Arpanet - Milnet

Re Arpanet "Sendmail" Virus attack November 3, 1988


Hi Gang!

It's now 3:45 AM on Wednesday 3 November 1988. I'm tired, so
don't believe everything that follows...

Apparently, there is a massive attack on Unix systems going on
right now.

I have spoken to systems managers at several computers, on both
the east & west coast, and I suspect this may be a system wide
problem.

Symptom: hundreds or thousands of jobs start running on a Unix
system bringing response to zero.

Systems attacked: Unix systems, 4.3BSC unix & variants (eg:
SUNs) any sendmail compiled with debug has this problem. See
below.

This virus is spreading very quickly over the Milnet. Within
the past 4 hours, I have evidence that it has hit >10 sites
across the country, both Arpanet and Milnet sites. I suspect
that well over 50 sites have been hit. Most of these are
"major" sites and gateways.

Method:

Apparently, someone has written a program that uses a hole in
SMTP Sendmail utility. This utility can send a message into
another program.
```

Unix-verkosta poimittu viesti kuvaa hyvin niitä sekavia tunnelmia, joita verkossa riehuva mato herätti.

sissa luultiin, että kyseessä oli vieraan valtion niitä vastaan suorittama hyökkäys.

Parin päivän kuluttua tilanne oli lopullisesti ohi, kun kaikki koneet oli saatu puhdistettua ja madot tuhottua. Sen jälkeen voitiin aloittaa jälkipyykin pesu. Koska Internet kattaa koko Yhdysvaltojen alueen, alkoi tutkimuksia hoitaa liittovaltion poliisi FBI.

Matoepidemian riehuessa pahimmillaan arveltiin, ettei sen tekijää saataisi koskaan kiinni. Madon alkuperä onnistuttiin kuitenkin jäljittämään parissa päivässä ja poliisi pidätti Morrisin. Omena ei ollut

pudonnut puusta pitkälle, sillä Robert Morrisin isä oli tunnettu tietoturva-asiantuntija.

Alkuvuodesta 1990 oikeus totesi Morrisin syyllistyneen rikokseen. Päätöksen pohjana oli vuonna 1986 annettu laki tietokoneiden väärinkäytöstä ja petoksesta. Lain sallima enimmäisrangaistus olisi ollut viisi vuotta vankeutta ja 250000 dollaria sakkoja. Kun tuomio vihdoin toukokuussa 1990 julistettiin, monet katsoivat Morrisin päässeen vähällä. Hän sai kolme vuotta ehdollista vankeutta, 10000 dollarin sakot ja 400 tuntia yhdyskuntapalvelua. Lieventäväksi asianhaaraksi katsottiin se, ettei Morrisin tarkoituksena ollut tuottaa suoranaista vahinkoa vaan ainoastaan osoittaa, miten helppoa madon levittäminen oli. Jos Morris olisi muuttanut ohjelmansa laskentakäskyt vaikkapa tiedostojen poistokäskyiksi, olisi mato saanut aikaan valtavat vahingot ja tuomiokin olisi ollut sen mukainen. Nyt mato voitiin vielä lukea kujeeksi - joskin hyvin vaaralliseksi.

Morrisin mato herätti asiantuntijat huomaamaan, miten haavoittuvia Internet-verkkoon kytketyt Unix-koneet todellisuudessa olivat. Aiemmin oli uskottu, että vain suojaamattomat mikrotietokoneet olisivat alttiita tämänkaltaisille hyökkäyksille. Unix-käyttöjärjestelmä oli jo 20 vuotta vanha, moneen kertaan kentällä testattu, mutta silti sen suojauksista löytyi madon mentäviä aukkoja. Unix-gurut kyllä tunsivat nämä aukot, mutta uskoivat, etteivät muut tienneet niistä eivätkä välittäneet korjata niitä.

Morrisin mato-ohjelma levisi koneesta toiseen elektronisena postina ja sen toiminta perustui Unixin postiohjelman puutteellisiin suojauksiin. Morrisin mato ei olisi toiminut mikroverkossa eikä kotikäyttäjän, joka lukee sähköpostia omalla mikrollaan, tarvitse pelätä saavansa matoa tai virusta postia lukiessaan.

Internetin tapaus sai runsaasti julkisuutta myös suomalaisissa tiedotusvälineissä. Niissä matoa tosin kutsuttiin virheellisesti virukseksi.

Troijan hevoset

Vanha taru kertoo, miten kreikkalaiset voittivat troijalaiset viekkautta käyttäen. Kun Troijan kaupunki osoittautui liian vahvaksi valloittaa,

rakensivat kreikkalaiset Odysseuksen neuvosta ison puuhevosen ja siirsivät sen yöllä kaupungin portille. Uteliaat troijalaiset siirsivät hevosen kaupunkiinsa tutkittavaksi, jolloin sen sisällä piilossa olleet soturit ryntäsivät ulos ja avasivat portit ulkona odottaville joukoille.

Yli 2000 vuotta myöhemmin Troijan hevoseksi alettiin kutsua ohjelmaa, jota hakkerit käyttivät murtautuessaan isoihin tietokoneisiin. Esikuvansa mukaisesti tällainen ohjelma näytti ulospäin houkuttelevalta ja viattomalta, mutta sen sisälle oli lisätty ylimääräinen ja käyttäjälle näkymätön pätkä koodia. Tämä koodi saattoi esimerkiksi pistää muistiin käyttäjän antaman tunnuksen ja salasanan ja välittää ne Troijan hevosen tekijälle.

Toinen tapa käyttää troijalaisia liittyi käyttäjän oikeuksien lisäämiseen. Troijalainen lisättiin jonkin sellaisen käyttäjän ohjelmaan, jolla oli esimerkiksi oikeus päättää muiden käyttäjien oikeustasoista ja muutenkin hallita järjestelmän toimintaa. Troijalainen kasvatti salaa tekijänsä oikeuksia tai kävi etsimässä levyllä olevan käyttäjärekisterin ja postitti sen tekijälleen tunnuksineen ja salasanoineen.

Mikrojen yleistyessä Troijan hevonen sai hieman toisen merkityksen. Troijalaiseksi alettiin kutsua ohjelmaa, joka nimensä perusteella näytti hyödylliseltä (esimerkiksi GAME.EXE), mutta joka käynnistettynä tekikin pelkkää vahinkoa esimerkiksi tyhjentämällä kiintolevyn.

Ensimmäinen PC:lle tehty troijalainen oli nimeltään EGABTR. Se lähti kiertämään käyttäjien keskuudessa heinäkuussa 1985. Mukana tullut ohje kertoi, että ohjelma parantaisi tuolloin yleisen CGA-näytön laatua uuden ja kalliin EGA-näytön tasolle. Ohjelma oli kuitenkin Troijan hevonen: heti käynnistyksen jälkeen se poisti kaikki kiintolevyn tiedostot ja tulosti vielä ruudulle pilkkaavan ilmoituksen "Arf, arf, Gotcha!".

Käyttäjältä toiselle leviävistä PD- eli julkisohjelmista löytyi monia Troijan hevosia. Pahimpia olivat tapaukset, joissa Troijan hevonen lisättiin johonkin tunnettuun julkisohjelmaan jälkikäteen. Alkuperäisen ja sabotoidun version pystyi erottamaan vain ohjelmatiedoston pituudesta.

Troijan hevonen tekee vahinkoa siinä missä viruskin. Viruksesta poiketen Troijan hevonen ei kuitenkaan lisäänny ts. se ei itse pyri levittämään itseään uusiin tiedostoihin. Troijalaisen sisältävä ohjelma

paljastuukin yleensä nopeasti ja jos tieto vahingollisesta ohjelmasta saadaan leviämään, osaavat muut käyttäjät välttää sitä.

Troijan hevoselle on joskus ehdotettu suomalaiskansallista vastinetta "kivileipä".

AIDS-troijalainen

Paljon maailmanlaajuista julkisuutta saanut troijalaistapaus sattui joulukuussa 1989. Tapahtumat lähtivät liikkeelle jo huhtikuussa 1989, jolloin kolme miestä perusti PC Cyborg Corporation-nimisen yrityksen Panamaan. Maanantaina joulukuun 11 päivänä 1989 yritys postitti Lontoosta käsin ainakin 7000, eräiden tietojen mukaan jopa 23000 levykettä osoitteisiin, jotka se oli saanut kahdesta eri lähteestä: osa oli ostettu PC Business World-lehden tilaajarekisteristä, osa koottu WHO:n lokakuussa 1988 Tukholmassa järjestämän AIDS-kongressin osanottajaluettelosta. Levykkeitä postitettiin lähinnä Eurooppaan, mutta myös Australia, Afrikka ja Aasia saivat osansa. Yhtään levykettä ei lähetetty Yhdysvaltoihin eikä tiettävästi myöskään Suomeen.

Levyke saapui vastaanottajalle valkoisessa kuoressa, jossa oli levykkeen lisäksi sininen paperi. Paperissa luki ohjelman nimi "AIDS Information Introductory Diskette Version 2.0" ja asennusohjeet. Niissä neuvottiin asettamaan levyke A: asemaan ja kirjoittamaan A:INSTALL. Paperin kääntöpuolella oli monimutkainen ohjelmalisenssi, jossa todettiin aluksi tavanomaiseen tapaan, ettei ohjelman tekijä ole vastuussa tuotteensa aiheuttamista vahingoista, mutta vihjattiin myös epäsuorasti ohjelman aiheuttamiin vahinkoihin ellei sen lisenssimaksua suoriteta. Kokeneet mikron käyttäjät ohittavat tällaiset tekstit nopealla vilkaisulla. Tässä tapauksessa se oli virhe.

Asennusohjelma kopioi AIDS.EXE-nimisen pääohjelman kiintolevylle, mutta loi samalla päähakemistoon myös kaksi näkymätöntä hakemistoa ja tallensi niihin omia piilotettuja työtiedostojaan. Kiintolevyn AUTOEXEC.BATiin lisättiin rivi, joka oli ovelasti naamioituna kasvatti troijalaisen käyttämää laskuria yhdellä aina kun kone käynnistettiin.

Kun laskuri oli ehtinyt arvoon 90 (eräät käyttäjät raportoivat muistakin arvoista), alkoi tapahtua. Ohjelma tulosti ruudulle ilmoituksen, jossa se kertoi suorittavansa 30 minuuttia kestävää operaatiota ja varoitti sammuttamasta konetta ennen kuin työ olisi tehty loppuun. Työn aikana ohjelma koodasi levyllä olevat tiedostonimet salakielelle ja sai aikaan vaikutelman, että levy oli muuttunut käyttökelvottomaksi. Ohjelmaan sisältyi myös osuus, joka neuvoi käyttäjää siirtämään ohjelman toiseenkin koneeseen ja näin levittämään vahinkoa.

Ensimmäiset levykkeet saapuivat vastaanottajilleen tiistaina 12.12.89. Osa asensi ohjelman heti käyttöön ja raportteja ohjelman vahingollisuudesta alkoi tihkua jo kahta päivää myöhemmin. Viikon päästä asia oli jo maailmanlaajuinen uutinen, mikä osaltaan vähensi vahinkojen määrää, sillä tieto ohjelman vaarallisuudesta tavoitti monet käyttäjät jo ennen kuin 90 käynnistyskertaa oli ehtinyt tapahtua. Osoitetiedot hyvässä uskossa myynyt PC Business World-lehti alkoi jakaa lukijoilleen nopeasti kehitettyä torjuntaohjelmaa AIDSOUT, joka poisti AIDS-ohjelman luomat piilotetut tiedostot tehden ohjelman vaarattomaksi. Tapaus osoittaa hyvin tietosuojalain tärkeyden. Osoiterekisteritkin voivat olla vaarallisia vääriin tai rikollisiin tarkoituksiin joutuessaan.

Vielä pari vuotta sitten AIDS-levyke olisi aiheuttanut paljon suuremmat vahingot. Uhrit eivät olisi osanneet epäillä levykkeitään eikä lehdistökään olisi kiinnostunut asiasta yhtä laajasti kuin nyt. Tietokoneviruksista ja Internetin madosta noussut kohu oli selvästi lisännyt käyttäjien valppautta.

Kaikkia AIDS-levykkeen taustoja ei ehkä koskaan saada selville. Tuhansien levykkeiden valmistaminen, postittaminen ja osoitetietojen hankkiminen tuli maksamaan arviolta 150000 dollaria, joten mistään kujeesta ei voinut olla kyse. Mikä siis oli PC Cyborgin lopullinen päämäärä? Oliko AIDS-levyke ansa, jota myöhemmin olisi käytetty kiristykseen? Aikoiko PC Cyborg tehdä toisen joukkopostituksen ja tarjota uhreille pelastuslevykettä sopivaksi katsomallaan hinnalla? Estikö tämän kohtalo, kun USA saman viikon lopulla hyökkäsi Panamaan, kaatoi kenraali Noriegan ja syöksi maan moniksi kuukausiksi sekasortoon? Vai laskiko yritys rikastuvansa jo niillä 189 ja 398 dollarin

summilla, joita käyttäjien pyydettiin lisenssiehdoissa maksamaan, mikäli aikovat käyttää ohjelmaa?

Helmikuun 1. päivänä 1990 FBI pidätti 39-vuotiaan, Clevelandistä kotoisin olevan Joseph Louis Poppin epäiltynä osallisuudesta levykkeiden lähettämiseen. Popp oli aiemmin työskennellyt WHO:n palveluksessa Etiopiassa ja Keniassa hoitaen juuri AIDS-tutkimukseen liittyviä asioita. Kuulusteluissa Popp myönsi osallistuneensa levykkeen valmistamiseen, mutta kielsi hyötyneensä työstä rahallisesti tai tienneensä sen haitallisista seurauksista. Kun Popp vetosi henkiseen sairauteensa, tuomari lähetti hänet mielentilatutkimukseen.

Pommit

Pommit ovat Troijan hevosten erikoistapauksia. Vahinkoa aiheuttava osuus on kätketty ohjelman sisään niin, että se aktivoituu vasta ohjelmoijan asettamien ehtojen täyttyessä. Jos ehdot liittyvät aikaan, ohjelmaa sanotaan aikapommiksi. Laukaisevana tekijänä voi olla myös jokin muu tekijä, kuten esimerkiksi levyn täyttöaste. Vahinkoa tuotetaan vasta sitten, kun levyn vapaa tila on laskenut ennalta-asetetun rajan alle. Näin varmistetaan, että levyn sotkeminen todella tuottaa vahinkoa.

Aikapommi voidaan ohjelmoida laukeamaan haluttuna päivänä, esimerkiksi perjantaina joka osuu kuukauden 13. päiväksi. Toinen suosittu valinta on aprillipäivä. Ohjelma voidaan tehdä myös niin, että se pitää kirjaa ajokertojen lukumäärästä. Aina kun ohjelmaa ajetaan, se käy kasvattamassa ohjelmakoodin seassa olevaa laskuria yhdellä. Lähes poikkeuksetta ohjelmia ajetaan nykyisin kiintolevyiltä, jolloin ohjelma voi helposti ja nopeasti muokata itse itseään. Levykkeellä ajettaessa kirjoitus kestäisi niin pitkään, että käyttäjä voisi huomata mitä on tekeillä ja kirjoitussuojatun levykkeen käyttäminen estäisi kirjoituksen kokonaan. Kiintolevyllä näitä ongelmia ei ole.

Vuonna 1988 maailmalla kiersi sitkeä huhu, jonka mukaan Larry I-pelin laittomasti kopioituun versioon olisi lisätty pommi, joka sotkisi kiintolevyn kun pelaajan pistemäärä ylittäisi 220 pistettä. Jopa maa, jossa pommiosuus oli peliin lisätty, tiedettiin: Hollanti. Koska Larry-

pelit ovat varmaan eniten kopioituja pelejä koko maailmassa, olisi tällainen versio levinnyt nopeasti. Jälleen yksi hyvä syy välttää laittomasti kopioituja pelejä!

Käyttäjän kannalta pommit ja viiveellä toimivat Troijan hevoset ovat erittäin kiusallisia. Ne ehtivät levitä pitkälle ennen kuin vahingon tekeminen alkaa ja vahingollisen ohjelman paljastaminen ennen sitä voi olla erittäin vaikeata. Ainoa tehokas lääke pommeja ja troijalaisia vastaan on tiedon levittäminen, jotta muut käyttäjät osaavat välttää niitä kantavia ohjelmia. Tässä mikroharrastajien purkit ja käyttäjäkokoukset ovat suureksi avuksi. Niissä liikkuu kokonaisia listoja (mm. "Dirty Dozen") ohjelmista, joiden on havaittu tuottavan vahinkoa joko tarkoituksella tai tahattoman ohjelmointivirheen seurauksena.

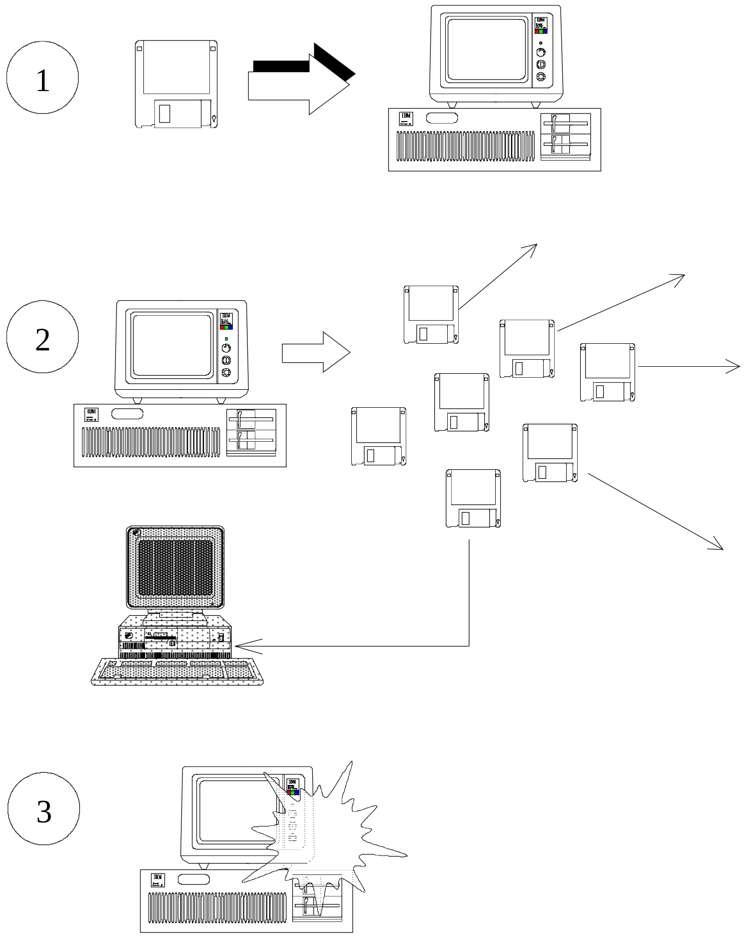
Virukset

Viimeisen tuholaisten ryhmän muodostavat varsinaiset tietokonevirukset. Pelottavasta nimestään huolimatta virus on vain pätkä ohjelmakoodia, jonka joku ohjelmoija on tehnyt. Termi "virus" kuulostaa maallikon korvissa pelottavalta, eikä olekaan ihme, että tietokoneviruksiin liittyy monia vääriä uskomuksia. Usein esimerkiksi kuvitellaan, että virukset syntyisivät itsestään tietokoneiden uumenissa. Todellisuudessa asia on täsmälleen päinvastoin: virukset ovat ihmisten tekemiä eivätkä ne suinkaan synny itsestään - itse asiassa virusten tekeminen on erittäin vaikeata.

Virus on ohjelmoitu niin, että se pyrkii levittämään itsestään kopioita toisiin tietokoneisiin. Virus leviää koneesta toiseen joko ohjelmatiedostojen tai levykkeiden välityksellä. Koska viruksen kantaja vaihtuu jatkuvasti, virukset leviävät nopeasti koneesta toiseen ja niiden alkuperää on vaikea jäljittää. Viruksiin ei jää tekijänsä sormenjälkiä.

Miten virus leviää?

Viruksen leviäminen tapahtuu kolmessa vaiheessa. Näistä ensimmäinen on tarttumisvaihe, jonka aikana virus pujahtaa uuteen tietokoneeseen ja piiloutuu sinne. Tartuntatapoja ja piilopaikkoja käsitellään



Viruksen elämän kolme vaihetta. Ensimmäisessä vaiheessa virus pääsee koneeseen levykkeen mukana. Toisessa vaiheessa virus leviää tekemällä itsestään kopioita niille levykkeille, joita koneessa käytetään. Näillä levykkeillä virus leviää nopeasti uusiin koneisiin. Kolmannessa vaiheessa virus iskee. Pahimmat virukset sotkevat käyttäjän kiintolevyn ja tuhoavat näin hänen tiedostonsa. Vaarattomammat virukset saattavat soittaa musiikkia koneen kaiuttimesta tai aiheuttaa muita yllätyksiä käyttäjälle. Eräistä viruksista kolmas vaihe puuttuu kokonaan: ne pyrkvitä vain lisääntymään ja leviämään eivätkä aiheuta suoranaista vahinkoa.

lähemmin seuraavassa luvussa.

Toinen vaihe on lisääntymisvaihe, jonka aikana virus pyrkii levittämään itsestään kopioita muihin koneisiin. Kun virustartunnan saaneessa koneessa käytetään levykkeitä, virus pyrkii kopioimaan itsensä niille. Jos kopiointi onnistuu, levittävät saastuneet levykkeet viruksen taas uusiin koneisiin.

Kolmannessa ja viimeisessä vaiheessa virus aktivoituu. Toisin kuin yleensä kuvitellaan, läheskään kaikki tietokonevirukset eivät aktivoituessaan tee suoranaista vahinkoa. Käytännön pilana virus voi esimerkiksi soittaa musiikkia koneen kaiuttimesta, tulostaa ylimääräisiä viestejä kuvaruudulle tai vaikkapa vilkuttaa näppäimistön merkkivaloja. Vakavampia ovat tapaukset, joissa virus sotkee kiintolevyn tai tuhoaa muulla tavoin käyttäjän tiedostot.

Tarttumiseen, lisääntymiseen ja vahingon tuottamiseen tarvittava koodi on puristettava mahdollisimman pieneen tilaan, jotta viruksen olisi helpompi piiloutua. Tyypillinen PC-virus on kooltaan vain 1-3 kilotavua. Tällaisen viruksen ohjelmointi on erittäin vaativa tehtävä ja se edellyttää syvällistä perehtymistä käyttöjärjestelmän toimintaan. Kuka tahansa kotitarveohjelmoija ei onneksi pysty viruksia tekemään.

Virukset mikroissa

Oikeat tietokonevirukset syntyivät vasta mikrotietokoneiden myötä. Asiaa oli tosin kokeiltu matojen muodossa jo isoilla tietokoneilla, mutta vasta mikrojen tuleminen loi pohjan todellisille tietokoneviruksille. Mikrot olivat halpoja, niitä oli paljon ja niiden ohjelmointiin käytetyt niksit olivat kaikkien tiedossa. Ensimmäisiä mikroviruksia olivat kaiketi jo 1980-luvun alussa Apple II:sta löydetyt tapaukset, jotka tosin matojen tapaan pyrkivät vain leviämään eivätkä tuottaneet suoranaista vahinkoa.

Kun PC:t ja Macit alkoivat yleistyä, löytyi viruksille vielä otollisempi kasvualusta. Nämä mikrot olivat entisiä paljon tehokkaampia ja niissä oli paljon Applen DOSia (huvittavaa kyllä, myös Apple II:n käyttöjärjestelmän nimi oli DOS ja sen yleisin versiokin oli 3.3) monipuolisempi käyttöjärjestelmä. Tästä syystä niille oli myös helpompi

tehdä viruksia. Myytyjen koneiden suuri määrä helpotti puolestaan virustartunnan leviämistä.

Ensimmäinen PC-virus löydettiin tammikuussa 1986. Mac-virukset ilmestyivät pian sen jälkeen. Aluksi uskottiin, että mikrovirukset olisivat vain lyhytaikainen villitys, joka menisi nopeasti ohitse. Näin ei kuitenkaan käynyt. PC-virusten määrä alkoi hiljalleen lisääntyä ja vuoden 1989 aikana se koki todellisen buumin, kun tunnettujen virusten määrä kasvoi lähes kaksinkertaiseksi.

Syrjäisen asemansa ansiosta Suomi välttyi pitkään viruksilta, sillä ensimmäiset laajemmat virustartunnat löydettiin Maceistä vasta vuoden 1988 aikana. PC:t saivat olla rauhassa tätäkin pidempään. Virusilmoituksia alkoi tulla vasta syksyllä 1989 - mutta silloin niitä tulikin sitten runsaasti.

Montako PC-virusta on olemassa?

Kukaan ei tarkkaan tiedä, montako erilaista tietokonevirusta on olemassa. Määrällisesti eniten viruksia löytyy PC-koneille, mutta sielläkin arviot vaihtelevat suuresti laskutavasta riippuen. Usein on vaikeata erottaa, milloin kyseessä on kokonaan uusi tietokonevirus ja milloin taas jonkin vanhan viruksen muunnos.

IBM:n viruslaboratorio oli tammikuun 1990 lopussa luokitellut 65 erilaista PC-virusta. Samaan aikaan eräät virusten torjuntaan tarkoitetut apuohjelmat mainostivat tuntevansa yli 140 virusta. Arvioiden väliset erot johtuvat erilaisesta luokittelutavasta. Kun jokaisesta viruksesta on liikkeellä vähintään kymmeniä, joskus jopa satoja tuhansia kopioita, on liikkeellä olevien virusten määrä laskettavissa miljoonissa.

Pahinta on, että uusia, ennestään tuntemattomia viruksia löydetään koko ajan. McAfee, jonka virusten etsintään tarkoitettu ohjelma on esitelty tässä kirjassa jäljempänä, ilmoitti kesäkuussa 1990 löytäneensä 17 uutta, ennestään tuntematonta viruslajia *yhden* kuukauden aikana!

Luonnolliset ja keinotekoiset virukset

Koneesta toiseen tarttuvaa ohjelmaa ei suotta kutsuta virukseksi. Ohjelmalla on suorastaan hämmästyttävän paljon yhteistä biologisen viruksen kanssa. Johtuvatko yhtäläisyydet siitä, että konevirukset ovat ihmisten tekemiä ja luonnon viruksissa käyttämä tekniikka paras mahdollinen matkittavaksi vai onko kyseessä jokin universaali laki energian säilymisen tai entropian lisääntymisen tapaan... niin, kukapa tietää?

Näkyvin samankaltaisuus luonnollisilla ja keinotekoisilla viruksilla on niiden tarve käyttää isäntää. Tietokonevirus on täysin vaaraton ellei sillä ole ohjelmaa tai käyttöjärjestelmää, johon kiinnittyä.

Myös solulla ja tietokoneohjelmalla on paljon yhteistä. Solun ohjelma sisältyy pitkään DNA-molekyyliketjuun ja siinä on tietokoneohjelman tavoin erikoismerkkejä, mm. loppumerkki. Kun solu jakautuu, tehdään alkuperäisestä DNA:sta kopio aivan samaan tapaan kuin tapahtuu tietokoneohjelmaa kopioitaessa. Solun DNA on ohjelmana uskomattoman monimutkainen. Se sisältää yhtä paljon tietoa kuin kuin 30-osainen tietosanakirja - ja tällaisia soluja on ihmisessä noin 10000 *miljardia*.

Jos kopioinnin aikana sattuu virhe, ei uusi yksilö ole enää alkuperäisen kaltainen. On syntynyt mutaatio. Yleensä tällaiset mutaatiot ovat elinkelvottomia ja kuolevat pois. Sama pätee tietokoneohjelmiin: jos bitit muuttuvat kopioinnissa, on uusi kopio lähes varmasti toimintakelvoton. Todennäköisyys sille, että virus muuttuisi kopiointivirheiden vuoksi uudenlaiseksi toimivaksi virukseksi on äärimmäisen pieni. Voi vain arvailla, miten monta kertaa tekstinkäsittelyohjelmaa pitäisi kopioida, ennen kuin se kopiointivirheiden vuoksi olisikin muuttunut taulukkolaskentaohjelmaksi...

Mutaatioita ja hieman toisistaan poikkeavia tietokoneviruksia tunnetaan lukuisia, mutta ne eivät suinkaan ole syntyneet sattumalta. Asialla ovat olleet ihmiset, jotka ovat ottaneet saamansa viruksen, muuttaneet sen ohjelmointia ja laskeneet viruksen jälleen eteenpäin. Tekemällä viruksista uusia versioita ja mutaatioita on pyritty vaikeuttamaan virusten etsintäohjelmien työtä.

Vaikein osa tietokoneviruksen ohjelmoinnissa on saada virus leviämään. Uuden yksilön synnyttäminen on vaikea ja monimutkainen prosessi riippumatta siitä, onko kyseessä elävä olento vai itseään kopioiva tietokoneohjelma. Luonnosta löytyy lukuisia esimerkkejä eläinlajeista, joiden lisääntymisrituaalin monimutkaisuus panee ihmettelemään, miten laji on voinut säilyä hengissä miljoonia vuosia. Eikä ihmisen lisääntyminenkään ole helppoa tai tuskatonta.

Solujen tapaan ohjelmat voivat olla immuuneja joillekin tietokoneviruksille. Tällöin ohjelmatiedoston rakenteessa on jotain sellaista, joka estää virusta tarttumasta siihen. Eräät virukset jättävät kaikkien pienimmät ja/tai isoimmat ohjelmatiedostot rauhaan. Osa viruksista pystyy puolestaan tarttumaan vain COM-tiedostoihin.

Eläimistä tai kasveista havaitut virukset ovat yleensä ihmiselle vaarattomia. Tietokonevirukset ovat yhtä tarkkoja elinympäristöstään. PC:lle tehty virus ei toimi pelimikrossa eikä Macin virus isossa tietokoneessa.

Tiedostoja ja levykkeitä voidaan "rokottaa" virusta vastaan. Analogia luontoon on jälleen ilmeinen. Rokottamisen idea perustuu siihen, että tiedostoon lisätään viruksen käyttämä merkki. Merkin nähdessään virus luulee jo tartuttaneensa ohjelman. Viruksen "heikennetty" versio lisää tiedoston "vastustuskykyä" ja estää todellisen virustartunnan.

Elämä sellaisena kuin me sen tunnemme perustuu hiilen kykyyn muodostaa monimutkaisia kemiallisia yhdisteitä. Hiilen lisäksi tällainen kyky on vain piillä, jota käytetään mikroprosessorien rakennusaineena. Kenties jossain päin maailmankaikkeutta onkin juuri piille rakentuvaa elämää. Piistä rakennettuja olioita uhkaavat mutaatioiden kautta syntyneet ykköstä ja nolla täynnä olevat piivirukset... tai sitten ei.

Mistä virukset tulevat Suomeen?

Koska tietokonevirukset leviävät nopeasti, on niiden alkuperää usein mahdotonta jäljittää. Jotain voidaan kuitenkin päätellä siitä, missä maassa virus ensiksi havaitaan. Uusia, ennestään tuntemattomia viruksia on löydetty mm. Hollannista, Länsi-Saksasta, Taiwanista, Israelista,

Uudesta Seelannista, Bulgariasta, Islannista, Italiasta sekä tietenkin USAsta. Virusten tekotaito näyttää levinneen yhtä laajalle kuin mikroharrastuskin eikä kunnioita mitään maantieteellisiä tai poliittisia rajoja. Jostain syystä Israelista ja Bulgariasta on löydetty poikkeuksellisen paljon uusia viruksia.

Useimmat virukset kulkeutuvat Suomeen saastuneiden levykkeiden välityksellä. Peliohjelmat saattavat kiertää koneesta toiseen ennen kuin päätyvät jonkun salkussa Suomeen. Tunnetaan myös tapauksia, joissa suomalaiset yritykset ovat saaneet virustartunnan ulkomaisen konttorinsa lähettämistä työlevykkeistä.

Pahimpia ovat tapaukset, joissa viruksen saastuttamia levykkeitä jakaa jokin mikroalalla toimiva laite- tai ohjelmavalmistaja. Tällaisista tapauksista on useita esimerkkejä.

Yleisesti uskotaan, että italialainen Ping-Pong -virus levisi Suomeen Olivetin omien huoltolevykkeiden mukana. Ennen kuin huolto huomasi mitä oli tapahtunut, se oli ehtinyt levittää tartuntaa moniin PC-koneisiin. Keväällä 1990 suomalainen iltapäivälehti kertoi viruksen aiheuttamasta epidemiasta eräässä valtion yrityksessä, mutta ei kertonut yrityksen nimeä.

Vuoden 1989 lopulla Suomeen tuli joukko Stoned-viruksen saastuttamia VGA-näytön apuohjelmalevykkeitä. Virus ehti levykkeiden mukana levitä useille käyttäjille ennen kuin asia havaittiin. Virus oli ilmeisesti pesiytynyt valmistajalla koneeseen jossa levykkeitä kopioitiin. Kesällä sama virus löydettiin Tecmarin VGA-korttien levykkeiltä.

Toukokuussa 1990 löysi eräs tarkkaavainen mikronkäyttäjä Vacsina-viruksen alkuperäiseltä, koneen mukana tulleelta DOS-apuohjelmalevykkeeltä. Kone ei ollut mikään halpaklooni vaan varsin tunnettua ja arvostettua merkkiä. Kun maahantuoja sai tiedon asiasta ja alkoi tutkia tapahtunutta, löytyi viruksen saastuttamia käyttöjärjestelmälevykkeitä useampia.

Eräs Singaporessa halpoja PC-kloonimikroja tehnyt valmistaja jakoi koneen mukana käyttöjärjestelmän lisäksi Artic mouse-levykettä. Levykkeiltä löytyivät sekä Disk Killer- että Jerusalem-virukset. Muutama suomalainenkin sai virukset käytyään ostamassa mikronsa Singaporesta.

Alkuvuodesta 1989 AMS-niminen Atari ST:lle ohjelmia tekevä valmistaja ilmoitti, että myyntiin oli päässyt erä viruksen saastuttamia Flair Paint-ohjelmia. Yritys ilmoitti vaihtavansa levykkeet maksutta uusiin. Vuotta myöhemmin sama tapahtui tunnetulle pelivalmistajalle Electronic Artsille. Nyt virus oli Atari ST:n Star Commander-pelissä. Levykkeet sai jälleen vaihtaa uusiin.

Näiden lähinnä laitetoimituksiin liittyvien tapausten lisäksi viruksia on havaittu myös eräistä vähemmän tunnetuista PC-valmisohjelmista.

Valmisohjelmien mukana levinneistä viruksesta tunnetuin on MacMagazine. Kanadalaisen MacMagazine-tietokonelehden päätoimittaja loi viruksen vuoden 1988 alussa tutkiakseen, miten nopeasti se leviäisi käyttäjien keskuudessa. Tulos ylitti kaikki odotukset. Virus nimittäin pujahti erään käyttäjän mukana Aldukselle, PageMaker-julkaisuohjelman tekijälle, ja heidän uuden Freehand-piirrosohjelman levykkeille. Kopiokoneet ehtivät monistaa saastuneita levykkeitä kolmen päivän ajan ennen kuin virus huomattiin. Tänä aikana levykkeet olivat löytäneet tiensä 5000 käyttäjälle. Kahdessa kuukaudessa ohjelma oli laittoman kopioinnin myötä levinnyt jo 350000 Maciin. Vaikuttava todiste siitä, miten tehokasta laiton kopiointi on!

Kaikeksi onneksi virus oli varsin harmiton. Huhtikuun 2 päivänä 1988, joka oli Macintosh II-koneen julkistamisen yksivuotispäivä, se tulosti kuvaruudulle viestin "Richard Brandow, Publisher of MacMag, and its entire staff Would like to take this opportunity to convey their UNIVERSAL MESSAGE OF PEACE To all Macintosh users around the world." ja tuhosi itse itsensä. Virus oli kouluesimerkki siitä, miten nopeasti virus voi laittoman kopioinnin seurauksena levitä.

Kuten edellä kerrotut tapaukset osoittavat, ei edes alkuperäisiin ohjelmalevykkeisiin voi aina luottaa. Tietoisuus viruksista on kuitenkin



MacMag oli ensimmäinen virus, joka levisi kaupasta ostetun ohjelman mukana. Sen jälkeen viruksia on löydetty muiltakin alkuperäislevykkeiltä.

lisääntynyt ja ainakin isommat ohjelmistotalot ovat alkaneet kiinnittää erityistä huomiota virusten torjuntaan. Monet PC-maahantuojat ovat niin ikään alkaneet tarkistaa säännöllisesti koneittensa mukana toimitettavia levykkeitä. Riski saada virus alkuperäisestä ohjelmapaketista on siten erittäin vähäinen, mutta kuitenkin aina olemassa.

Jonkin verran viruksia pääsee maahan myös tietoliikenneyhteyksien mukana. Kuka tahansa harrastaja voi soittaa modeemin välityksellä lähes minne tahansa maapalloa ja siirtää linjaa pitkin muutamassa minuutissa itselleen ohjelmia. Ohjelmiin mahdollisesti tarttuneet virukset leviävät tällä tavalla maanosasta toiseen.

Virukset leviävät ällistyttävän nopeasti. Hyvänä esimerkkinä on Yankee Doodle-virus, joka havaittiin ensi kertaa Wienissä syyskuun lopulla 1989. Jo paria kuukautta myöhemmin virus oli ehtinyt saastuttaa Suomessa useita mikroja.

Miksi viruksia tehdään?

Miksi sitten viruksia tehdään? Kuka viitsii kuluttaa aikaansa monimutkaisen viruksen laatimiseen kun tietää, ettei työstä voi koskaan vaatia itselleen kunniaa? Päinvastoin, viruksen tekijän on pidettävä suunsa tiukasti kiinni. Joskus aivan harmittaa se kekseliäisyys ja työmäärä, joka virusten tekemiseen on tuhlattu. Maailma voisi olla parempi paikka, jos nämäkin resurssit olisi käytetty parempiin tarkoituksiin.

Suurin viruksia laativa ryhmä lienevät 15-25 vuotiaat pojat. Heille virusten tekeminen on hakkeroinnin tapaan älyllinen haaste, josta tulee erityisen jännittävä siksi, että se on kiellettyä. Viruksia tehdään, koska halutaan nähdä miten ne toimivat. Tämä selittää sen, miksi niin monet virukset tuottavat erilaisia jekkuja tai piloja yrittämättäkään tehdä varsinaista vahinkoa.

1990-luvun Vaahteramäen Eemeli on poika, joka harrastaa mikron käyttöä ja on tietoliikenteen kautta yhteydessä muihin alan harrastajiin. Hän voi esittää kysymyksiä muille, jotka kokeilevat samoja asioita. Tietoverkon kautta se käy helposti, vaikka vastaajat olisivat toisella mantereella. 1800-luvun alussa hän pisti uteliaisuuttaan päänsä soppakulhoon - nyt hän on yhtä utelias mikron suhteen. Nuoren iän ei pidä

antaa hämätä, sillä monet parhaista ohjelmoijista ovat alle 20-vuotiaita. Internetin madon tekijä oli 23-vuotias. Vain tämän ikäinen pystyy edes keksimään moisia kujeita. Vanhemmille ohjelmoijille ne eivät tulisi mieleenkään.

Kokonaan uuden viruksen kehittäminen on vaikeata. Helpommalla pääsee, kun ottaa kiinni jonkin olemassa olevan viruksen, tekee siihen hieman muutoksia ja pistää viruksen eteenpäin. Esimerkiksi laajalle levinneestä Jerusalem-viruksesta on tällä tavoin tehty lukuisia eri versiota. Tuntemattomat ohjelmoijat ovat myös "parannelleet" alkuperäisiä viruksia korjaamalla niissä olleita virheitä ja rajoituksia.

Miehiseen tapaan tehdä tiedettä on aina kuulunut asioiden tutkiminen niiden itsensä vuoksi. Asioille ei tarvitse olla pitäviä perusteluita tai hyviä syitä. Mount Everestille kiivettiin, "koska se oli olemassa". Atomipommi tehtiin, koska haluttiin testata toimisiko näkymättömistä atomeista laaditut teoriat myös käytännössä. Tekoälyä tutkitaan siitä huolimatta, että toteutuessaan se saattaa aiheuttaa suuria ja arvaamattomia yhteiskunnallisia mullistuksia. Näiden tutkimuskohteiden rinnalla virusten tekeminen tuntuu harmittomalta näpertelyltä.

Viruksia syntyy toki muutoinkin kuin vain nykyajan Eemelien kujeina. Vain muutaman syntyhistoria tunnetaan yksityiskohtaisemmin. Macin nVir-niminen virus luotiin kesällä 1987 kokeilumielessä hollantilaisella nuortenleirillä. Opettaja halusi näyttää, miten tehdään ohjelma, joka piiloutuu ja käynnistyy ennalta-annettuna päivänä. Leirin jälkeen ohjelmat ja dokumentit tuhottiin, mutta silti muutaman kuukauden kuluttua ilmestyivät ensimmäiset tällä periaatteella tehdyt virukset.

Eräissä tapauksissa viruksia on pyritty käyttämään myös modernina tapana vaikuttaa asioihin. Joulukuussa 1987 havaittiin Jerusalemin yliopistossa virus, joka levisi nopeasti ympäri maailmaa. Viruksen analyysi paljasti, että se oli ohjelmoitu aktivoitumaan perjantaina, joka osui kuukauden 13. päiväksi. Seuraava tällainen päivä sattui olemaan toukokuussa 1988 ollut Israelin 40-vuotispäivän aatto. New York Times päätteli viruksen olevan poliittinen protesti ja siitä lähtien virusta alettiin kutsua PLO-virukseksi. Mitään yhteyttä PLOn ja viruksen välillä ei kuitenkaan koskaan löydetty. USAn presidentin vaalikampanjan aikana kehitetty Macintoshin Dukakis-virus kuuluu samaan sarjaan. Se tulosti kuvaruudulle ilmoituksen "Dukakis for president!".

Vuoden 1989 lopulla NASA laukaisi avaruuteen Galileo-luotaimen. Ympäristöaktivistit yrittivät estää laukaisun vedoten luotaimessa olevan ydinreaktorin turvallisuusriskeihin, mutta se ei auttanut. NASA laukaisi luotaimen vastustuksesta huolimatta, mutta eivätpä vastustajatkaan jääneet neuvottomiksi. Itseään nimellä Worms Against Nuclear Killer kutsuva ryhmä ujutti NASAn tietokoneverkkoon madon, joka tulosti käyttäjien kuvaruuduille ydinvoiman vastaisia iskulauseita. Mato saastutti noin 60 DECin tietokonetta NASAn omassa verkossa ja levisi verkon kautta myös Sveitsiin CERNin tutkimuskeskukseen.

Viruksia on joskus käytetty myös koston ja kiristyksen muotona. Macintoshin Scores-viruksen uskotaan syntyneen potkut saaneen ohjelmoijan kostona entiselle työnantajalleen Electronic Data Systemsille. Pian potkujen jälkeen yritykseen saapui nimetön levyke, jolta Scores-virus alkoi maaliskuussa 1988 levitä maailmanlaajuisesti.

Kuka hyötyy viruksista?

Dekkareissa syyllinen löytyy usein tutkimalla, kuka hyötyi eniten murhasta. Voisikohan samaa periaatetta soveltaa tietokoneviruksiin? Kuka hyötyy tietokoneviruksista? Tuskin muut kuin valmisohjelmien tekijät.

He ovat jo vuosia katselleet voimattomina, miten kalliisti tuotetut ohjelmat ovat levinneet laittomina kopioina maapallon ympäri. Laittomasti kopioidun AutoCAD-suunnitteluohjelman hinta kaukoidän tietokonekaupassa on tuhat markkaa. Suomessa saman ohjelman virallinen myyntihinta on 35000 markkaa. Ei ole ihme, jos valmistajat ovat vihaisia.

Aikoinaan kopiointia yritettiin estää lisäämällä ohjelmiin kopiosuojauksia. Suojaukset oli kuitenkin mahdollista kiertää ja ne tuottivat ongelmia myös sellaisille käyttäjille, jotka olivat ostaneet ohjelman oikealla rahalla. Näiden ongelmien vuoksi ostajat alkoivat karttaa kopiosuojattuja ohjelmia ja ostivat mieluummin kilpailevan ohjelman, jos siinä ei ollut suojausta. Lopulta kaikki valmistajat luopuivat hankaliksi ja tehottomiksi osoittautuneista suojauksista.

Viruksista noussut kohu on vähentänyt laitonta kopiointia paljon tehokkaammin kuin parhaatkaan kopiosuojaukset. Ohjelmantekijöiden kannalta on siis vain hyväksi, että käyttäjien viruspelkoa pidetään yllä ja ruokitaan sopivasti. Samaan joukkoon kuuluvat tietenkin myös virusten torjuntaohjelmien tekijät ja myyjät. Tällaisten ohjelmien markkinat ovat syntyneet vasta virusten yleistymisen myötä, mutta niiden kaupallinen merkitys on jäänyt vähäiseksi. Parhaat ohjelmat kun ovat usein ilmaisia PD-ohjelmia.

Mitään todisteita ohjelmatalojen sekaantumisesta virusten tuottamiseen ei tietenkään ole, mutta teoria kuulostaa varsin uskottavalta...

2

Virus lähikuvassa

Tässä luvussa tarkastellaan lähemmin tietokoneviruksen toimintaa: miten se tarttuu koneeseen, mihin se piiloutuu ja mitä se voi tehdä. Vaikka esimerkkinä on jälleen PC ja DOS-käyttöjärjestelmä, toimivat kaikki virukset samalla periaatteella. Viruksen toiminnan ymmärtäminen edellyttää myös jonkin verran PC-tekniikan tuntemusta. Lukija, joka ei ole kiinnostunut mikron tekniikasta, voi huoletta hypätä yli siitä kertovat kohdat.

Virusten luokittelu

Kun tiede alkaa tutkia uutta aluetta, on ensimmäinen työvaihe perinteisesti ollut havaintojen luokittelu. Luomalla karsinat ja jakamalla havainnot niiden perusteella saadaan asioihin jonkinlainen järjestys ja helpotetaan niiden ymmärtämistä.

Mikrotietokoneista löydetyt virukset voidaan jakaa kolmeen ryhmään niiden leviämistavan mukaan:

- tiedostovirukset
- levykevirukset
- sovellusohjelmavirukset

Ensimmäisen ryhmän muodostavat tiedostovirukset, jotka leviävät koneesta toiseen tarttumalla ohjelmatiedostoihin. Kun viruksen saanut ohjelma käynnistetään, virus pääsee muistiin ja kopioi itsensä uusiin

ohjelmiin. Tiedostovirukset voivat levitä ohjelmatiedostojen mukana koneesta toiseen myös lähiverkon tai modeemiyhteyden välityksellä.

Toisen ryhmän muodostavat levykevirukset, jotka eivät tarvitse isäntäohjelmaa. Ne piiloutuvat levyllä alueille, joilla normaalisti sijaitsee vain käyttöjärjestelmän omaa tietoa. Tältä alueelta virus pääsee muistiin heti, kun kone käynnistetään. Leviäminen on mahdollista vain levykkeiden välityksellä.

Kolmannen ja samalla pienimmän ryhmän muodostavat sovellusohjelmien virukset. Nämä virukset on tehty sovellusohjelman omalla makro- tai ohjelmointikielellä ja ne leviävät vain kyseisen ohjelman sisällä piiloutuen sen tekemiin työtiedostoihin. Lotuksen, Excelin, Wordin ja WP:n kaltaisten ohjelmien käyttämä makrokieli on niin monipuolista, että sillä olisi mahdollista tehdä myös viruksia. Erityisen vaarallisia ovat makrot, jotka käynnistyvät automaattisesti kun ohjelma käynnistetään tai kun jokin työtiedosto avataan. Tällainen virus voi kopioida itsensä jokaiseen käytettävään työtiedostoon ja näin levittää itseään.

Esimerkki sovellusviruksesta on Macin Dukakis-virus. Se leviää Hypercard-ohjelman pinoissa ja mainostaa Dukakista presidentiksi.

Miten virus leviää?

Koska virus on vain pätkä ohjelmaa, sen on päästävä mikron työmuistiin (RAMiin) voidakseen toimia. Työmuistissa sijaitsevat normaalisti käyttöjärjestelmä ja sovellusohjelma. Virus tunkee itsensä vapaaksi jääneeseen osaan työmuistia ja kiinnittyy sinne.

Virus ei voi levitä levykkeeltä toiselle fyysisen kosketuksen tai muun vastaavan välityksellä. Virus voi levitä tietoliikenteen kautta, mutta vain silloin, kun siirretään viruksen saastuttamia ohjelmatiedostoja. Pelkkä modeemi tai lähiverkko ei sinänsä voi levittää virusta.

Levyllä oleva virus on täysin vaaraton jono ykkösiä ja nollia. Tällaisesta levystä voi huoletta katsoa DIR-listauksen, levyä voi tutkia erilaisilla ohjelmilla ja tiedostoja voi jopa kopioida levyltä toiselle.

Virus alkaa toimia vasta päästyään työmuistiin ja saatuaan prosessorin suorittamaan omaa koodiaan. Keskusmuistiin pääsemiseen on kaksi

eri tapaa. Virus voi ladata itsensä muistiin käyttöjärjestelmän mukana heti kun kone käynnistetään. Tämä edellyttää, että virus on kiinnittynyt levyllä alueille, joita alkulataukseen käytetään. Alueet ovat normaalien tiedostoalueiden ulkopuolella ja koska niiden sisältö ei näy esimerkiksi DIR-komennolla, ovat ne virusten kannalta hyviä piilopaikkoja.

Toinen tapa on livahtaa muistiin jonkin sovellusohjelman mukana. Kun sovellus haetaan levyltä muistiin ja käynnistetään, käynnistyy ensiksi sovelluksen perässä roikkuva virus. Virus jää muistiin ja vasta sen jälkeen käynnistetään itse sovellus.

Kolmas mahdollisuus on tarttua suoraan levyllä olevaan tiedostoon, jolloin viruksen ei tarvitse piiloutua Kun viruksen sisältävä ohjelma käynnistetään, virus etsii levyltä jonkin uuden ohjelman ja tarttuu siihen. Tällainen virus leviää kahta ensimmäistä tapaa hitaammin, mutta sitä on vaikeampi huomata, koska virus ei missään vaiheessa jää muistiin.

Keskusmuistissa piileskelevän viruksen on helppo levitä. Muistissa ollessaan se voi esimerkiksi tutkia jokaisen levykkeen, joka A: asemaan laitetaan ja kopioida itsensä sille. Jos kyseessä on ohjelmiin tarttuva virus, se voi tartuttaa jokaisen ohjelman, jota koneessa ajetaan. Mikään ei estä virusta tarttumasta myös työtiedostoihin, esimerkiksi taulukkolaskentamalliin tai tekstinkäsittelyn dokumenttiin. Näin ei kuitenkaan kannata tehdä, sillä prosessori ei koskaan aja työtiedostossa olevaa koodia eikä virus tästä syystä voi päästä muistiin.

Viruskoodi kirjoitetaan yleensä prosessorin omalla ohjauskielellä, konekielellä. Vain sitä käyttämällä saadaan viruksesta tarpeeksi pienikokoinen. Koska erilaiset tietokoneet käyttävät erilaista konekieltä, eivät yhdelle konetyypille tehdyt virukset toimi toisella koneella. Esimerkiksi Macin virukset eivät toimi PC:ssä ja päinvastoin. Mikrovirukset eivät myöskään toimi isoissa koneissa, joten pelko siitä että virukset leviäisivät pääteyhteyden myötä keskuskoneeseen on turha.

Periaatteessa olisi mahdollista tehdä virus, joka pystyisi toimimaan useassa eri koneessa. Viruksen pitäisi sisältää oma koodi jokaista prosessoria ja käyttöjärjestelmää varten tai sitten sen pitäisi pystyä ohjelmoimaan itse itsensä uutta ympäristöä varten. Vaikka tällaisen viruksen tekeminen olisikin teoriassa mahdollista, tulisi viruksesta epäkäytännöllisen iso ja tehoton.

Mihin virus piiloutuu?

Kun virus pääsee järjestelmään, on sen ensimmäinen tehtävä piiloutua. Macintoshin käyttöjärjestelmässä piilopaikkoja on selvästi PC:tä enemmän, koska Mac graafisena ympäristönä eristää käyttäjän tehokkaasti laitetekniikasta ja levyjen teknisistä yksityiskohdista.

PC:n DOS-käyttöjärjestelmä on yksinkertaisempi ja paljon karumpi. Siksi myös piilopaikkoja on vähemmän. Monilla PC-käyttäjillä ei ole mitään graafista käyttöliittymää, vaan he näkevät levyn täysin paljaana. DOS ei edes yritä peitellä levyn todellista tilannetta.

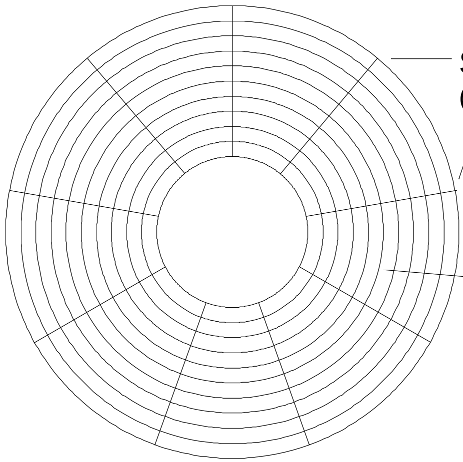
Piilopaikkoja kuitenkin löytyy, kunhan niitä vain osaa etsiä. Piilojen ymmärtämiseksi on tunnettava hieman PC:n käyttämien levyjen rakennetta.

Mistä on pienet levyt tehty...?

Kaikissa tietokoneissa käytettävät levyt toimivat periaatteessa samalla tavalla. Kuoren sisällä on pyöreä levy, jonka tallennuspinta on jaettu samankeskeisiin uriin (tracks). Niitä leikkaavat säteen suuntaiset sektorit (sector). Mitä useampi sektori levyllä on, sitä kapeampia viipaleita ne leikkaavat levystä. Sektorin leikkaamaa kohtaa yhdeltä uralta kutsutaan PC:ssä lohkoksi (block). Englanninkieliset termit menevät tässä pahemman kerran ristiin, sillä sanalla "sector" tarkoitetaan sekä levyn sektoria että yhtä sen lohkoa. Esimerkiksi termi "bad sector", joka tarkoittaa levyllä olevaa viallista lohkoa, pitäisi oikeastaan olla "bad block". Vika on lohkossa, ei kokonaisessa sektorissa.

Sektorien ja urien määrä vaihtelee levykkeen tyypistä riippuen. Vanhat 360-kilon levykkeet ("lerput") tallensivat levylle 40 uraa 9:ään sektoriin. Levystä käytettiin molemmat puolet, joten lohkoja oli kaikkiaan 40 * 9 * 2 = 720. Jokaiseen lohkoon mahtuu aina puoli kiloa eli 512 tavua tietoa. Tästä levykkeen kapasiteetiksi saatiin 720 * 1/2 eli 360 kilotavua.

IBM AT:ssä otettiin vuonna 1984 käyttöön 1,2 megatavun levykkeet. Niissä levyn pinta oli jaettu 80 uraan ja 15 sektoriin, joista saatiin



Kaikki levyt koostuvat sektoreista ja urista. Näiden leikkauskohtaan muodostuu yksi 512 tavun lohko, jota englanniksi kutsutaan harhaanjohtavasti sanalla "sector".

80 * 15 *2 * 512 eli 1228800 tavua. Muutamaa vuotta myöhemmin yleistyneet 3,5-tuumaiset kovat levykkeet ("korput") rakennettiin samalla periaatteella joko 720-kiloisiksi tai 1,44-megaisiksi.

Kiintolevyillä käytetään samaa periaatetta. Koska levyt eivät ole pehmeitä vaan kovaa metallia, voidaan niitä pinota useita päällekkäin ja jokaiselle antaa oma luku/kirjoituspäänsä. Metallin ansiosta levyt laajenevat lämmetessään hyvin vähän joten urat voidaan tehdä paljon

Levy	koko	uria	sekt.	puol.	kapasiteetti	DOS-versio
180 kt	5,25"	40	8	1	163840	DOS 1.0
320 kt	5,25"	40	8	2	327680	DOS 1.1
360 kt	5,25"	40	9	2	368640	DOS 2.0
1,2 Mt	5,25"	80	15	2	1228800	DOS 3.0
720 kt	3,5"	80	9	2	737280	DOS 3.2
1,44 Mt	3,5"	80	18	2	1474560	DOS 3.3

DOSin tuntemat levykeformaatit ja DOS-versio, jossa se on otettu käyttöön. Ensimmäinen levykeformaatti oli yksipuolinen; sen jälkeen levykkeistä on aina käytetty molemmat puolet.

kapeammiksi ja sijoittaa lähemmäksi toisiaan kuin levykkeillä. Tyypillisellä kiintolevyllä on 600-1000 uraa. Sektoreita on yleensä 17, mutta uusissa levyissä määrä saattaa olla suurempikin. Kun levyjä on vielä 2-4 päällekkäin on helppo ymmärtää, miksi kiintolevyn kapasiteetti on niin paljon levykettä suurempi.

Varatut alueet

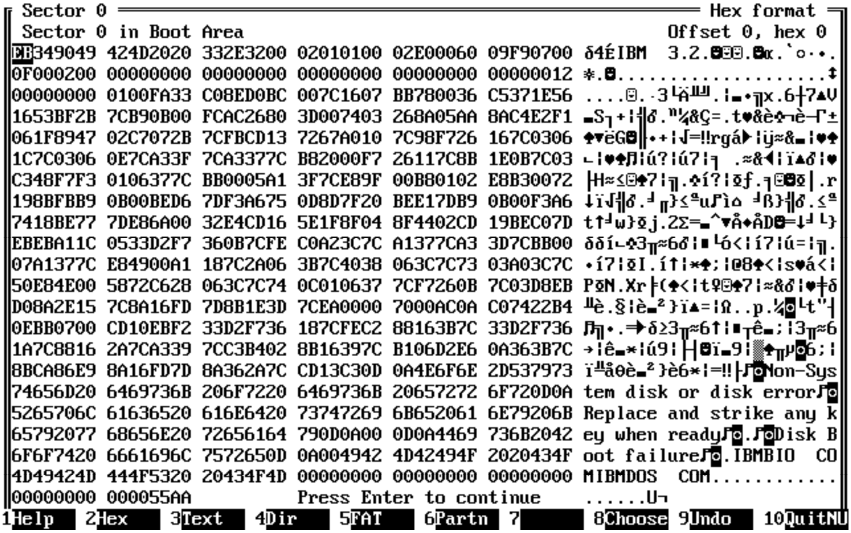
Osa levyn tallennuskapasiteetista on käyttäjän ulottumattomissa. Käyttöjärjestelmä varaa tilaa itselleen mm. pitääkseen kirjaa levyllä vapaina olevista alueista. Jokaisella levyllä, olipa kysessä sitten lerppu, korppu tai kiintolevy, on ainakin seuraavat neljä varattua aluetta:

Käynnistyslohko

Yksi lohko levyn alusta on varattu aloitusta varten. Kun mikro käynnistetään, käyttöjärjestelmä käy lukemassa käynnistyslohkon (boot sector) sisällön. Lohko kertoo levyn tekniset tiedot (mm. urien määrän ja varattujen alueiden koon) sekä sisältää pienen ohjelman, joka yrittää aloittaa käyttöjärjestelmän latauksen. Ellei levylle ole siirretty käyttöjärjestelmää, tämä ohjelma huomaa asian ja tulostaa virheilmoituksen. Koska virheilmoitus tulee levyltä eikä varsinaisesta käyttöjärjestelmästä (koska sitä ei vielä ole ladattu), voi ilmoituksen kieli poiketa koneessa olevan DOS-version kielestä. Vaikka koneessa olisi englanninkielinen DOS-versio, voi ilmoitus tulla vaikkapa saksaksi tai suomeksi jos levyke on aikanaan alustettu näitä kieliä käyttävällä FORMAT-ohjelmalla.

FAT 1 ja FAT 2

FAT on lyhenne sanoista File Allocation Table. Osuva suomenkielinen käännös "tilanvaraustaulukko" kertoo hyvin mistä on kyse. FAT pitää kirjaa levyn käytöstä: se kertoo, mikä kohta levystä on vapaana ja mikä ei. Iso tiedosto saattaa olla useana palasena eri puolilla levyä jolloin



Käynnistyslohkon alusta löytyy tunnus, joka kertoo millä DOS-versiolla levy on alustettu (esimerkissä IBM PC-DOS 3.2). Tämän jälkeen tulevat levyn tekniset parametrit sekä käynnistyksessä tarvittava konekielinen ohjelma. Lohkon lopussa näkyvät virheilmoitukset tulostuvat ruudulle, mikäli alkulataus ei jostain syystä onnistu.

FAT kertoo, missä järjestyksessä palaset pitää lukea ja missä ne sijaitsevat.

FAT on levyn toiminnan kannalta elintärkeä. Jos taulukon tiedot menevät sekaisin, ei levyllä oleviin tiedostoihin enää päästä käsiksi. Koska FAT on näin tärkeä, pidetään sitä levyllä kahtena samanlaisena kappaleena. Toinen toimii alkuperäisen varmuuskopiona. Kun levyä käytetään, kirjoittaa DOS välittömästi tiedot molempiin FATeihin. Valitettavasti käyttöjärjestelmä ei itse osaa ottaa varmuuskopiota käyttöön, jos alkuperäiselle sattuu jotakin. CHKDSK-ohjelma ei edes huomaa, jos FATeissa on eroja. Levyä käytetään aina ykkös-FATin mukaan.

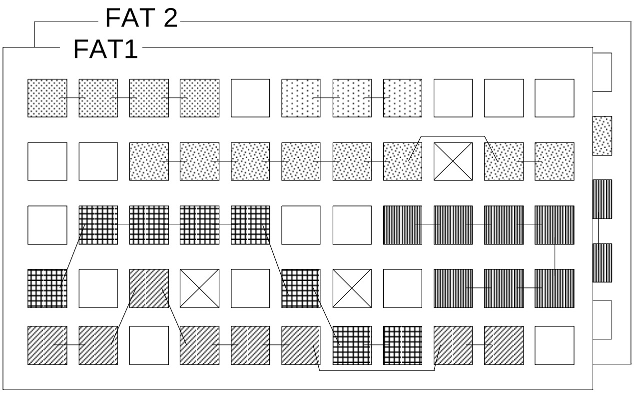
FATin käyttämä tapa vapaan tilan seurantaan on kaikessa yksinkertaisuudessaan nerokas. FATit vievät levykkeeltä vain muutaman lohkon ja kiintolevyltäkin vain muutama kymmenen lohkoa. Näin pienessä tilassa ne pystyvät pitämään kirjaa koko levyn tilankäytöstä.

FAT-järjestelmä sopiikin erittäin hyvin levykkeille ja kohtalaisesti myös normaalikokoisille kiintolevyille. Erittäin isoilla levyillä FAT alkaa tuhlata kohtuuttomasti tilaa eikä se muutenkaan sovellu esim. vaativaan verkkokäyttöön. OS/2:ssa onkin mahdollista käyttää myös tehokkaampaa HPFS-järjestelmää, jossa on korjattu useimmat FAT-järjestelmän puutteet.

FAT-järjestelmän suurin heikkous on sen haavoittuvuus. Virus tai troijalainen pystyy nollaamaan koko FATin muutamassa sekunnissa, jolloin levyn tiedostoja ei enää voida käyttää. Tämä on paljon tehokkaampi ja nopeampi tapa tuottaa vahinkoa kuin kiintolevyn alustaminen.

Päähakemisto ja osiotaulukko

Viimeisen osan levyn varatuista alueista muodostaa päähakemisto (root directory). Päähakemisto luodaan levyn alustamisen yhteydessä ja sille varataan aina kiinteän mittainen tila levyn alusta. Kohdasta, jossa päähakemisto päättyy, alkaa varsinainen käyttöjärjestelmä. Koska päähakemiston koko on kiinteä, mahtuu päähakemistoon vain rajattu määrä tiedostoja. Kiintolevyillä tämä määrä on yleensä 512 tiedostoni-



FATin alkiot muodostavat ketjuja, joita seuraamalla päästään lukemaan itse tiedostoja. FAT on tärkeä, koska tiedoston osat saattavat sijaita eri puolilla levyä. FATissa olevat valkoiset alueet tarkoittavat tyhjää kohtaa levyllä. Vika-alueet (bad sector) on merkitty FATiin rastilla, jotta DOS osaisi kiertää ne.

meä. Jotta levylle voitaisiin tallentaa useampia tiedostoja on käytettävä alihakemistoja.

Alihakemistot rakentuvat samalla periaatteella kuin päähakemistokin, mutta DOSin kannalta ne ovat tavallisten tiedostojen kaltaisia. Ne voivat sijaita missä kohtaa levyä tahansa ja ne voivat myös kasvaa dynaamisesti. Alihakemistossa ei siten ole tiedostojen kappalemääräistä rajoitusta.

Kiintolevyllä on edellisten lisäksi vielä yksi varattu alue. Tämä alue sijaitsee kiintolevyn uloimmalla uralla. Koska urien numerointi aloitetaan ulkoreunalta, kutsutaan tätä uraa nollauraksi.

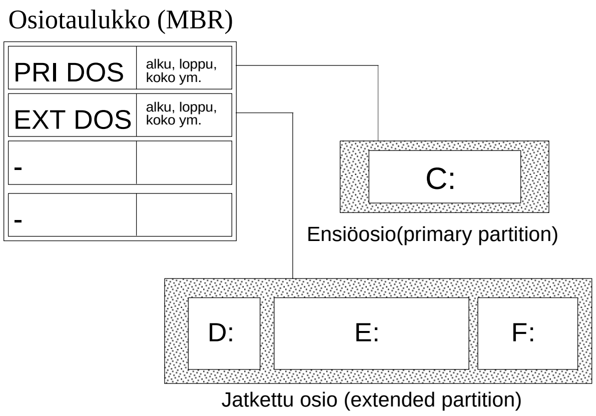
Kiintolevy voidaan FDISK-ohjelman avulla jakaa enintään neljään täysin itsenäiseen osioon (partition). Yleensä kaikki tila varataan DOS-käyttöön, jolloin osiotaulukon kolme viimeistä riviä ovat tyhjiä. Nollauran ensimmäinen lohko on nimeltään osiotaulukko (Master boot record, MBR). Tässä lohkossa sijaitseva taulukko kertoo, miten kiintolevyn osiojako on tehty: mistä osiot alkavat ja miten isoja ne ovat.

Aina DOS 3.2:een asti DOS pystyi käyttämään vain yhtä osiota. Koska osion koko ei voinut ylittää 32 megatavua, ei DOS 3.2:lla voinut käyttää tätä isompia kiintolevyjä. Eräät laitevalmistajat tosin lisäsivät tämän kyvyn omaan DOS-sovitukseensa, mutta alkuperäisessä IBM:n ja Microsoftin versiossa sitä ei ollut.

Kun isot kiintolevyt yleistyivät, oli pakko keksiä kiertotie 32 megatavun ylitse. DOS 3.3:ssa voidaankin käyttää kahta osiota, ns. ensiöosiota (primary partition) ja jatkettua osiota (extended partition). Ensiöosio näkyy C: asemana ja myös jatkettu osio on jaettava asematunnuksiin (ns. loogisiin levyasemiin) ennen kuin sitä voidaan käyttää. Mikään asematunnuksista ei kuitenkaan voi olla yli 32 megatavua.

DOS 4.0:ssa 32 megatavun raja poistettiin lopullisesti. Tämän ansiosta isokin kiintolevy voidaan ottaa käyttöön yhtenä ainoana C: tunnuksena, jolloin osiotaulukosta tarvitaan vain yksi rivi. Loput kolme jäävät yleensä tyhjiksi.

Osiotaulukkoon merkitään myös, mikä määritellyistä osioista on aktiivinen ts. mistä käyttöjärjestelmä ladataan kun kone käynnistetään. Vain yksi osio voi olla kerrallaan aktiivinen, eikä se koskaan voi olla DOS 3.3:n jatkettu osio, koska osio on jaettava asematunnuksiin.



Osiotaulukkoon mahtuu neljä riviä, joista enintään kaksi ensimmäistä voidaan käyttää DOSilla. Taulukko kertoo, miten levyn osiojako on tehty. DOS 3.3:ssa ensimmäinen osio (ensiöosio) voi olla kooltaan enintään 32 megatavua. Jatkettu osio on jaettava loogisiin asematunnuksiin, joista minkään koko ei voi olla yli 32 megatavua. DOS 4.0:sta lähtien isokin levy voidaan ottaa käyttöön yhtenä isona C: asemana, mutta turvallisuussyistä näin ei yleensä kannata tehdä.

Taulukon lisäksi lohkossa sijaitsee käynnistyslohkon kaltainen pieni ohjelmapätkä, joka hyppää aktiiviseksi merkityn osion käynnistyslohkoon ja käynnistää sieltä varsinaisen käyttöjärjestelmän latauksen.

Taulukko ja pieni ohjelma mahtuvat yhteen lohkoon. Jos levyllä on 17 sektoria, jäävät loput 16 lohkoa käyttämättä. Yleensä ne ovat täynnä nollaa tai jotakin muuta toistuvaa numerokoodia. Eräät levyohjaimet saattavat tallentaa tälle alueelle omaan toimintaansa liittyviä parametreja.

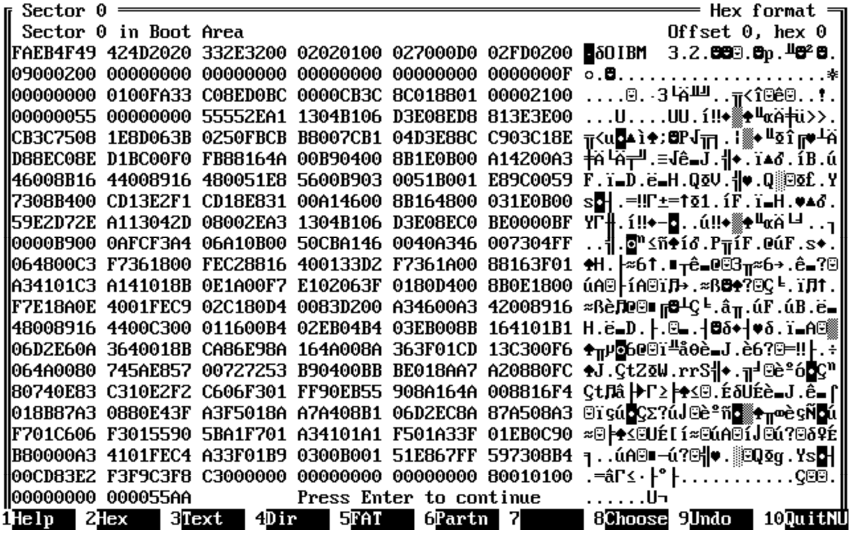
Viruksen kanssa piilosilla

Edellä kuvattiin levyn teknistä rakennetta. Seuraavaksi tarkastellaan, miten virus pystyy näitä alueita käyttämään, miten piiloutuminen tapahtuu ja miten viruksen voi havaita.

Käynnistyslohko

Levyn käynnistyslohkoon tarttuvia viruksia ovat mm. Disk Killer, Italialainen ja Stoned. Lohkoa on helppo käyttää, koska sekä levykkeen että kiintolevyn lohkot ovat saman tapaisia ja sijaitsevat levyn alussa. Virus korvaa lohkon lopussa olevan latausohjelman omalla koodillaan ja pääsee näin muistiin heti kun mikro käynnistetään.

Käynnistyslohkon käyttöön liittyy eräitä ongelmia. Ensinnäkin lohko on vain 512 tavun mittainen ja siitäkin osa on varattu levyn teknisille tiedoille. Näin ahtaaseen paikkaan mahtuu vain osa viruksesta, joten loppu pitää sijoittaa jonnekin muualle. Yleensä loppu kirjoitetaan levylle normaaliin tapaan ja kohta naamioidaan tämän jälkeen bad sectoriksi. Alkuperäistä käynnistysohjelmaakaan ei pidä unohtaa, sillä ilman sitä mikro ei käynnisty. Kopio alkuperäisestä käynnistyslohkosta sijoitetaan yleensä samaan piiloon viruksen loppuosan kanssa. Kun käynnistyslohkossa oleva viruskoodi on ajettu ja virus saatu muistiin,



Disk Killer-viruksen saastuttama käynnistyslohko. Virus on muuttanut alussa olevaa hyppyosoitetta (FAEB) osoittamaan omaa koodiaan, jonka se on kirjoittanut alkulatauskoodin paikalle. Kopio alkuperäisestä lohkosta on piilotettu levylle luotuun bad sectoriin.

hypätään alkuperäiseen käynnistysohjelmaan ja aloitetaan käyttöjärjestelmän lataaminen normaaliin tapaan.

Keskusmuistiin päästyään virus pyrkii tekemään itsestään kopioita. Kun A: asemaan laitetaan uusi levyke ja annetaan jokin levyä käyttävä komento (pelkkä DIR A: riittää), tarkistaa virus onko levyke jo saanut tartunnan. Ellei ole, virus käy siirtämässä alkuperäisen käynnistyslohkon turvaan ja kopioi itsensä sen paikalle. Kaikki tämä käy muutamassa sekunnissa eikä käyttäjä yleensä huomaa, että mitään epänormaalia on tekeillä. Jos levyke on kirjoitussuojattu, ei virus tietenkään pysty kopioimaan sille itseään. Riippuu viruksen ohjelmoinnista, osaako se lopettaa tartuntayritykset hallitusti vai pysähtyykö se virheilmoitukseen "Write protected error", joka riittää paljastamaan viruksen asioista perillä olevalle käyttäjälle.

Jos virus on piiloutunut levykkeen käynnistyslohkoon, se voi levitä koneesta toiseen, vaikkei levykkeellä olisi käyttöjärjestelmää eikä yhtään ohjelmatiedostoa. Leviäminen tapahtuu silloin, kun käyttäjä unohtaa levykkeen A: asemaan. Kun virta seuraavan kerran kytketään päälle, mikro yrittää käynnistystä levykkeeltä ja ajaa siinä olevan käynnistysohjelman. Ruudulle tulostuu virheilmoitus "Not a system disk" eikä mikro käynnisty. Käynnistyslohkossa ollut ohjelma on kuitenkin jo ehtinyt kopioida itsensä kiintolevylle ja kun mikro seuraavan kerran käynnistetään kiintolevyltä, pääsee virus keskusmuistiin.

Bad sector

Tietoa siitä, mitkä kohdat levystä ovat viallisia eivätkä kelpaa tallentamiseen, pidetään FATeissa. Virus voi kopioida itsensä levylle ja käydä merkitsemässä FATiin, että viruksen kohdalla oleva alue on viallinen. Virus saa olla levyllä kaikessa rauhassa, sillä käyttöjärjestelmä kiertää vialliseksi merkityn alueen.

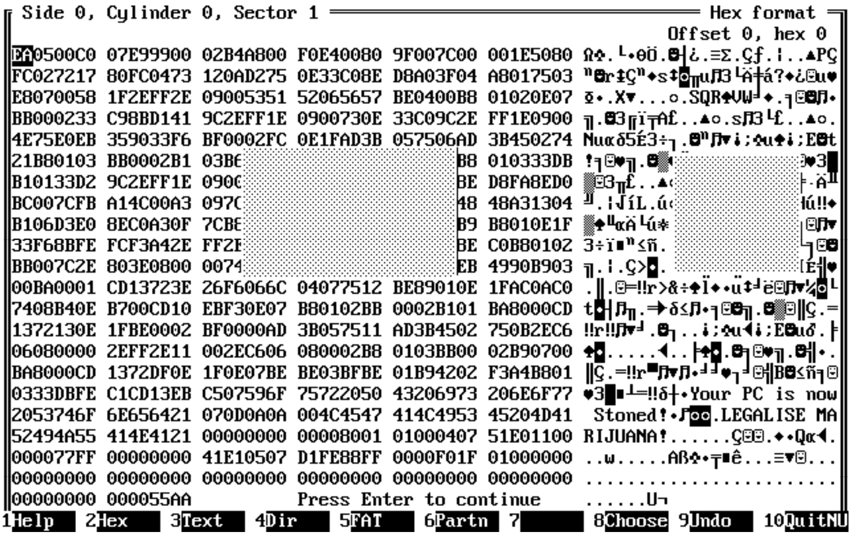
Jos koko virus sijaitsisi bad sectorissa, ei se pääsisi ikinä keskusmuistiin. Osan viruksen koodista pitääkin olla joko ohjelmatiedostossa tai esimerkiksi käynnistyslohkossa. Kun alkuosa ajetaan, se hakee loput itsestään bad sectorista ja siirtää kaiken keskusmuistiin.

Bad sectoriin piiloutuva virus on helppo havaita, sillä CHKDSK-ohjelma lukee FATin ja tulostaa siellä olevien bad sector-merkintöjen lukumäärän.

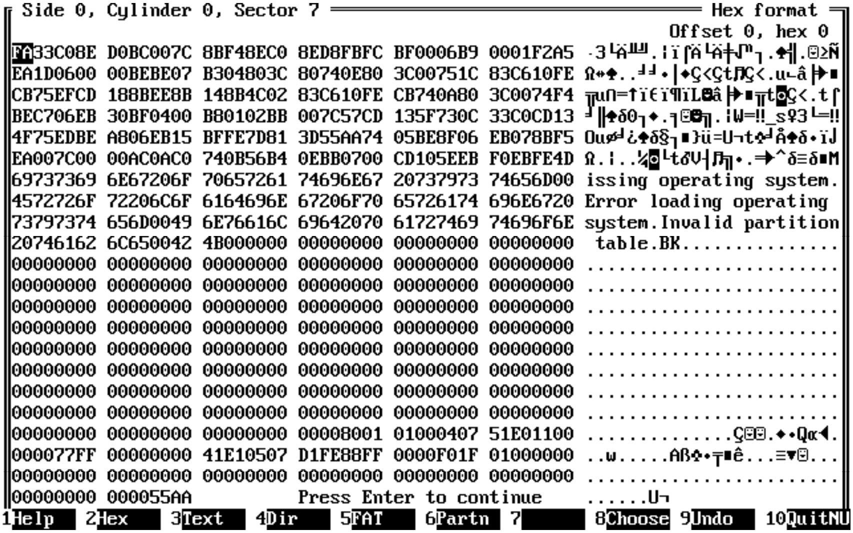
Nollaura ja sisimmät urat

Uloin nollaura koostuu 512 tavun mittaisesta osiotaulukosta ja tyhjästä tilasta. Stoned-virus korvaa ensimmäisessä lohkossa olevan latausohjelman omalla koodillaan ja siirtää alkuperäisen osiotaulukon lohkoon numero seitsemän.

Nollauran tyhjä alue muodostaa oivallisen piilopaikan viruksille, koska mikään DOSin komennoista ei "näe" sinne. Tyhjää tilaa on ainakin 16 lohkoa (8 kiloa) - monissa kiintolevyissä enemmänkin, koska niissä on yli 17 sektoria. Virukselle kannalta tilaa on enemmän kuin tarpeeksi. Kiintolevyn nollauraa käyttävät piilopaikkanaan mm. Disk Killer ja Stoned-virus. Nollauralle tarttunutta virusta on vaikeata poistaa, koska edes FORMAT-ohjelma ei tyhjennä sitä.



Stoned-virus piiloutuu osiotaulukkoon. Koska koko virus mahtuu 512 tavun lohkoon, on osa koodista sensuroitu näkymättömiin.


```
Side 0, Cylinder 0, Sector 7                                    Hex format
                                                              Offset 0, hex 0
FA33C08E D0BC007C 8BF48EC0 8ED8FBFC BF0006B9 0001F2A5
EA1D0600 00BEBE07 B304803C 80740E80 3C00751C 83C610FE
CB75EFCD 188BEE8B 148B4C02 83C610FE CB740A80 3C0074F4
BEC706EB 30BF0400 B80102BB 007C57CD 135F730C 33C0CD13
4F75EDBE A806EB15 BFFE7D81 3D55AA74 05BE8F06 EB078BF5
EA007C00 00AC0AC0 740B56B4 0EBB0700 CD105EEB F0EBFE4D
69737369 6E67206F 70657261 74696E67 20737973 74656D00  issing operating system.
4572726F 72206C6F 6164696E 67206F70 65726174 696E6720  Error loading operating
73797374 656D0049 6E76616C 69642070 61727469 74696F6E  system.Invalid partition
20746162 6C650042 4B000000 00000000 00000000 00000000   table.BK..............
00000000 00000000 00000000 00000000 00000000 00000000  ........................
00000000 00000000 00000000 00000000 00000000 00000000  ........................
00000000 00000000 00000000 00000000 00000000 00000000  ........................
00000000 00000000 00000000 00000000 00000000 00000000  ........................
00000000 00000000 00000000 00000000 00000000 00000000  ........................
00000000 00000000 00000000 00000000 00000000 00000000  ........................
00000000 00000000 00000000 00000000 00000000 00000000  ........................
00000000 00000000 00000000 00000000 00000000 00000000  ........................
00000000 00000000 00000000 00008001 01000407 51E01100
000077FF 00000000 41E10507 D1FE88FF 0000F01F 01000000
00000000 00000000 00000000 00000000 00000000 00000000  ........................
00000000 000055AA          Press Enter to continue
1Help  2Hex  3Text  4Dir  5FAT  6Partn  7  8Choose  9Undo  10QuitNU
```

Alkuperäisen osiotaulukon Stoned-virus siirtää nollauran seitsemänteen sektoriin. Taulukko kertoo, mistä osiot alkavat ja minkä kokoisia ne ovat. Lisäksi lohkosta löytyy pieni latausohjelma sekä virheilmoitukset, jotka tulostetaan ruudulle ellei osiotaulukkoa pystytä käynnistyksen aikana lukemaan.

Helpon, mutta epäluotettavan piilon virukselle tarjoavat levyn sisimmät, viimeiset urat. Ne otetaan käyttöön vasta levyn tullessa täyteen. Useimmiten levykkeellä on aina jonkin verran tyhjää tilaa, jossa virus voi piileskellä. Virallisten 40 uran lisäksi on 360 kilon levykkeillä mahdollista käyttää kolmea epävirallista lisäuraa, numeroita 40..42. Niitä on joskus käytetty myös levykkeiden kopiosuojaukseen, koska uria ei voi kopioida tai käyttää normaalin DOSin keinoin. Lisäurille piiloutuva virus on varmassa suojassa eikä se näy mitenkään.

Päähakemisto

Päähakemiston koko vaihtelee levyn tyypistä riippuen. Pienimmillään hakemiston koko on 360 ja 720 kilon levykkeillä (112 nimeä), joilla hakemisto mahtuu 7:ään lohkoon (3,5 kilotavua). Kiintolevyllä 512 nimen tallentamiselle varataan 32 lohkoa (16 kilotavua).

Päähakemisto on tuskin koskaan aivan täynnä. Yleensä hakemiston lopussa on aina jonkin verran käyttämätöntä tilaa, kiintolevyn päähakemistossa todennäköisesti paljonkin. Kaikki ohjeet kun neuvovat jättämään päähakemiston mahdollisimman tyhjäksi ja sijoittamaan tiedostot alihakemistoihin. Virus voi piiloutua hakemiston loppuun, mutta paikka ei ole kovin turvallinen. Jos käyttäjä päättääkin kopioida lisää tiedostoja päähakemistoon, kirjoittuvat nimitiedot viruksen koodin päälle ja virus tuhoutuu.

Stoned-virus korvaa käynnistyslohkon omalla koodillaan ja kopioi alkuperäisen lohkon 360 kilon levykkeillä päähakemiston viimeiseen lohkoon. Jos päähakemistoon kopioidaan riittävä määrä tiedostoja, virus tuhoutuu. Kiintolevyllä virus piiloutuu nollauralle, jossa se on paljon paremmassa turvassa.

Alihakemistoihin ei kannata piiloutua, sillä DOS kohtelee niitä tavallisten tiedostojen tavoin. Kun hakemisto perustetaan, DOS varaa sille tietyn määrän nimiä. Tämä määrä käy nopeasti pieneksi käyttäjän kopioidessa siihen tiedostoja, jolloin DOS käy kasvattamassa tilaa tarpeen mukaan. Päähakemistosta poiketen alihakemistoon mahtuvilla nimillä ei ole teoreettista ylärajaa. Ainoa, joka määrää rajoittaa, on levyn vapaa tila.

Pieni keskeytys

Miten virus sitten pystyy vaikuttamaan koneen toimintaan? Keskusmuistissa oleva virus ei vielä sellaisenaan pysty vaikuttamaan mikron toimintaan. Viruksen pitääkin käyttää apunaan käyttöjärjestelmän palveluita.

Kun mikrossa ajettava sovellus haluaa lukea tai kirjoittaa koneessa olevaa levyasemaa, se ei itse käynnistä moottoria eikä ohjaa lukupäätä. Sovelluksista tulisi kohtuuttoman isoja ja monimutkaisia, jos ne joutuisivat huolehtimaan kaikista yksinkertaisistakin asioista itse. Omatoimisuuden sijaan sovellukset luottavat käyttöjärjestelmään ja välittävät pyyntönsä sille.

Koneessa olevan BIOS ROMin ja DOS-käyttöjärjestelmän palveluita kutsutaan keskeytyksillä (interrupt). Kun sovellusohjelma haluaa

kutsua käyttöjärjestelmän palveluita, se ei suinkaan hyppää suoraan muistiosoitteeseen josta palvelu alkaa. Hyppy saattaisi toimia yhdessä DOS-versiossa, mutta seuraavassa versiossa kyseinen palvelu voisi jo olla aivan toisessa kohtaa muistia.

Suoran hypyn sijaan ohjelma suorittaa keskeytyksen. Intelin prosessoreissa on mahdollista määritellä 256 erilaista keskeytystä, jotka numeroidaan 16-kantajärjestelmän mukaisesti 00..FF. Koska 256 erilaista keskeytystä ei vielä riitä kaikkien palvelujen tarjoamiseen, on useita palveluita ryhmitelty saman keskeytyksen alle. Kun keskeytys tehdään, määrää prosessorin AH-rekisterissä oleva koodiarvo sen, mikä palveluista (function) valitaan. Eniten palveluita tarjoaa keskeytys numero 21: peräti 105 erilaista (DOS 4.0-versiossa). Osalla näistä on vielä omia alipalveluita (subfunctions).

Keskeytykset 00..07 kuuluvat prosessorille itselleen. Niillä reagoidaan esimerkiksi nollalla jakamiseen (keskeytys 00) ja Shift-PrtSc-näppäimen painallukseen (keskeytys 05). Keskeytykset 08..1F liittyvät oheislaitteiden, kuten COM-porttien ja näppäimistön käyttöön. Alimpien keskeytysten palveluosoitteet löytyvät koneen BIOS ROMista.

DOSin tarjoamat palvelut alkavat keskeytyksestä numero 20. Alkuperäisessä PC:ssä keskeytykset 40..7F olivat käyttämättä, mutta uudemmissa malleissa niillekin on varattu omia palveluita. Suurin osa keskeytyksistä 80..FF on kokonaan käyttämättä tai sitten eri sovellukset (erityisesti lähiverkot ja DOSin moniajolaajennukset) varaavat niitä omaan käyttöönsä ajon aikana. Ongelmia syntyy, jos sekä virus että ajettava sovellus yrittävät varata itselleen samaa keskeytystä.

Muistiosoite, josta keskeytyksen takana oleva palvelu alkaa, löytyy aivan RAM-muistin alusta. Jokaiseen 256 keskeytykseen liittyy neljän tavun mittainen osoite, joka osoittaa joko koneen RAM- tai ROM-muistiin. Keskeytysten osoitetaulukko vie siten 1024 tavua tilaa. Kun kone käynnistetään ja DOS ladataan muistiin, käytetään tätä kilotavua tilapäisenä työalueena. Määrittelemättömät 80..FF-numeroiset keskeytykset saattavat siten sisältää satunnaisia arvoja.

Keskeytysten käytöllä taataan se, ettei sovellusta tarvitse muuttaa vaikka käyttöjärjestelmän versiota vaihdetaankin. Uudessa DOS-versioissa keskeytysten numerointi ja toiminta ovat ennallaan, mutta niitä vastaavat palvelut löytyvät eri kohdista muistia. Keskeytyksillä on

toinenkin etu: sovellusohjelma voi vaihtaa keskeytykseen liittyvää palveluosoitetta siten, että BIOS ROMin tai DOSin palvelu korvataan ohjelman tarjoamalla paremmalla palvelulla.

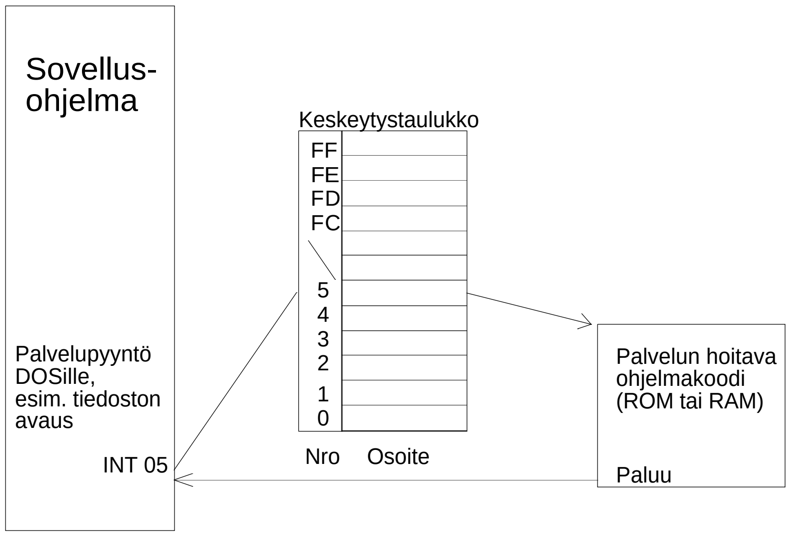
Hyvän esimerkin keskeytyksen käytöstä antaa GRAPHICS-ohjelma. Kun käyttäjä painaa Shift+PrtSc -näppäinyhdistelmää, tapahtuu keskeytys 05. Normaalisti keskeytys osoittaa koneen BIOS ROMiin (esimerkkikoneessa F000:FF54). Tässä kohtaa ROMia on pieni rutiini, joka kopioi näytöllä olevat merkit yksi kerrallaan LPT1-kirjoitinporttiin ja palaa takaisin.

ROM-rutiini osaa kopioida vain tekstimerkkejä eikä ymmärrä mitään ruudulla näkyvästä grafiikasta. Jotta grafiikankin tulostaminen olisi mahdollista, pitää RAM-muistiin ladata tätä varten GRAPHICS-ohjelma. Jäätyään muistiin se siirtää keskeytyksen 05 osoittamaan itseään (esimerkkikoneessa DOS 4.0:lla osoitteeksi tuli 1681:0460). Kun Shift+PrtSc -näppäintä painetaan, ohjelma aktivoituu ja muuttaa kuvaruudulla näkyvän grafiikan kirjoittimelle sopivaksi. Grafiikan tulostamista ei ole laitettu valmiiksi ROMiin, koska tulostus vaihtelee näyttölaitteesta ja kirjoittimesta riippuen. ROMissa olevaa koodia ei voisi muuttaa uusille kirjoittimille ja näyttölaitteille sopivaksi.

Virus noudattaa samaa tekniikkaa. Keskusmuistiin päästyään se kiilaa itsensä sovelluksen ja keskeytyspalvelun väliin muuttamalla keskeytyksen osoittamaan ensin itseensä. Vasta kun virus on tarkistanut, voiko se käyttää tehtyä kutsua hyväkseen, välitetään kutsu alkuperäiseen palveluosuuteen. Jos sovellus esimerkiksi pyytää tietoja A: aseman levykkeeltä, pääsee virus käyttämään levyä ensimmäisenä. Se voi kopioida itsensä levykkeelle ja välittää vasta sitten keskeytyksen alkuperäiseen palveluosoitteeseen.

Tärkein DOSin käyttämistä keskeytyksistä on 21, jolla tehdään useimmat tiedostojen käsittelyssä tarvittavat toimet. Varastamalla tämän keskeytyksen itselleen virus pystyy ohjaamaan tiedostojen käsittelyä haluamallaan tavalla ja mm. kopioimaan itsensä käynnistettävän tiedoston perään.

Keskeytysten avulla virus pystyy hallitsemaan järjestelmää lähes esteettä. Hyvänä esimerkkinä tästä on Brain-virus, joka tarttuu levyn lukemisessa käytettävään keskeytykseen. Virus on piilossa käynnistyslohkossa, mutta jos jokin ohjelma (esimerkiksi virusten etsintäohjelma)

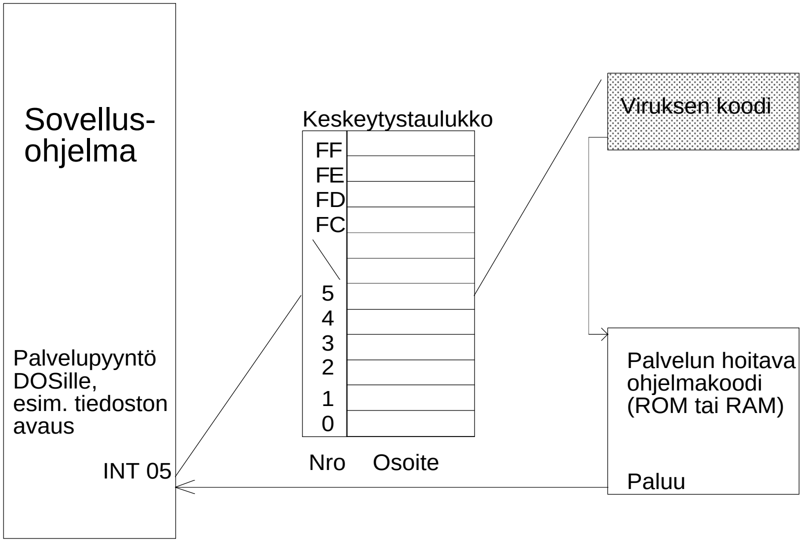


Kun sovellus haluaa käyttöjärjestelmän palvelua, se suorittaa keskeytyksen (esimerkissä INT 05). Palvelun osoite haetaan keskeytystaulukosta ja tämän osoitteen perusteella hypätään muistissa oikeaan kohtaan. Kun palvelu päättyy, ajovuoro palautuu jälleen alkuperäiselle ohjelmalle.

pyytää lohkoa luettavakseen, virus antaakin tilalle alkuperäisen bad sectoriin piilotetun lohkon eikä etsintäohjelma huomaa mitään! Jos tällainen virus pääsee muistiin, ei viruksia levyltä etsivästä ohjelmasta ole mitään hyötyä. Nähdäkseen todellisen käynnistyslohkon etsintäohjelman pitäisi ohittaa DOSin palvelut kokonaan ja ohjata suoraan levykeaseman moottoria ja lukupäätä.

Virusten muuttamia keskeytysosoitteita voi käyttää myös niiden paljastamiseen. Luvussa seitsemän kerrotaan ohjelmista, jotka käyvät lukemassa keskeytysosoitteiden arvot ja vertaavat niitä aiemmin saatuihin. Jos osoitteet eivät täsmää, on keskeytystä peukaloitu. Ongelmaksi jää erottaa, milloin asialla on ollut virus ja milloin laillinen ohjelma.

Keskeytysten varastaminen on yksi syy virusten aiheuttamiin epämääräisiin ongelmiin. Jos virus varaa itselleen saman keskeytyksen mitä sovelluskin käyttää, voivat seuraukset olla hyvinkin yllättäviä.

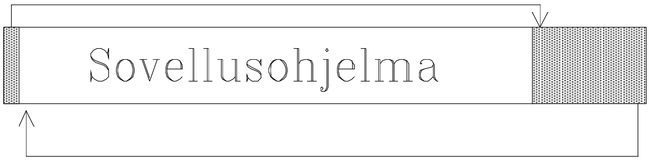


Virus asettaa keskeytyksen osoittamaan ensin itseensä. Vasta kun se on tutkinut, voiko keskeytystä käyttää sen omiin tarpeisiin, ohjataan keskeytys alkuperäiseen palveluosoitteeseen.

Tiedostovirukset

Toisiin ohjelmiin tarttuva virus ei joudu kuluttamaan aikaa piilopaikan keksimiseen. Se kopioi itsensä ohjelmatiedoston loppuun (joskus myös alkuun) ja käy säätämässä alkuperäisen ohjelman koodia siten, että myös virusosuus ajetaan ennen varsinaisen ohjelman ajoa. Tällaisen viruksen tekeminen on helpompaa kuin piiloutuvan viruksen, mutta se on myös helpompi huomata. Viruksen tarttuminen ohjelmatiedostoon näkyy heti DIR-listassa, koska tiedoston pituus kasvaa.

DOSissa käytetään kahta erilaista ohjelmatiedostoa. COM-tyyppiset tiedostot ovat teknisesti yksinkertaisia ja yleensä kooltaan alle 64 kiloa, joten viruksen on helppo tarttua niihin. EXE-tiedostojen rakenne on monimutkaisempi ja se voi jopa vaihdella. Esimerkiksi Windows- ja OS/2-ohjelmien EXE-tiedostot poikkeavat sisältä katsottuna perus-



Kun virus (harmaa osa) tarttuu ohjelmaan, se kopioi oman koodinsa ohjelmatiedoston loppuun. Ohjelman alkuun lisätään virukseen osoittava hyppykäsky, jotta virus tulee ajettua heti kun ohjelma käynnistetään. Vasta kun virus on ajettu, siirtyy ajovuoro alkuperäiselle ohjelmalle.

DOSin EXE-tiedostoista. Tästä syystä viruksetkaan eivät osaa tarttua niihin.

COM- ja EXE-tiedostoihin tarttuminen tapahtuu eri tavoin. Muutamat viruksista ovat erikoistuneet siten, että ne tarttuvat vain jompaan kumpaan tyyppiin - yleensä yksinkertaisempaan COMiin. Tällainen on esimerkiksi 1701/1704-virus, jonka tarttumista tarkastellaan seuraavassa hieman lähemmin. Uhrina on 8 tavun mittainen ohjelmatiedosto, joka tulee Procomm Plussan mukana. DIR-komento kertoo ohjelmasta seuraavaa:

```
C>DIR CODE.COM

CODE     COM         8 01.01.80    0.48
        1 tiedosto(a).Vapaana   11649024 tavua.
```

Koska COM-ohjelma on konekielistä koodia, ei sen toimintaa voida suoraan nähdä mistään. Koodia voidaan kuitenkin tutkia muuttamalla se DEBUGin avulla symboliselle konekielelle:

```
C>DEBUG CODE.COM
-u 100
1986:0100 B400          MOV AH,00
1986:0102 CD16          INT 16
1986:0104 B44C          MOV AH,4C
1986:0106 CD21          INT 21
```

Komento U on lyhenne sanasta Unassemble ja tarkoittaa muunnosta konekielestä symboliselle konekielelle (assemblerille).

Ohjelman ensimmäinen komento lataa AH-rekisteriin arvo nolla. Toisella rivillä kutsutaan keskeytystä numero 16. Tässä, samoin kuin jatkossakin, on kaikki lukuarvot ilmaistu DEBUGin käyttämässä 16-kantaisessa lukujärjestelmässä.

Keskeytys numero 16 liittyy näppäimistön käsittelyyn. AH-rekisterissä oleva numerokoodi kertoo tarkemmin, mitä keskeytyksessä tehdään. Numero 02 esimerkiksi pyytää keskeytystä palauttamaan tiedon sellaisten erikoisnäppäinten kuin Ctrl, Alt ja Caps Lock painamisesta. Esimerkin käyttämä koodi nolla pyytää keskeytystä palauttamaan merkkipuskurissa olevan painalluksen ASCII- ja scan-koodin arvot. Scan-koodi palautetaan AH-rekisterissä ja ASCII-arvo AL-rekisterissä.

Kolmannella rivillä AH-rekisteriin ladataan arvo 4C ja seuraavalla rivillä kutsutaan keskeytystä 21. AH-rekisterin arvosta riippuen se suorittaa mitä erilaisempia tehtäviä alkaen tiedostojen käsittelystä ja päätyen kellonajan asettamiseen. Numero 4C on lopetuskoodi, joka lopettaa ohjelman siten, että käyttöjärjestelmään palaa ERRORLEVEL-arvona rekisterin AL sisältö.

Tutkimus osoittaa, miten yksinkertainen ohjelma CODE.COM on. Tämän lyhyempää ohjelmaa tuskin voisi edes tehdä. Käynnistyksen jälkeen ohjelma jää odottamaan näppäimen painallusta ja palauttaa sen ASCII-koodin ERRORLEVEL-muuttujassa takaisin käyttöjärjestelmään. Todellisissa sovellusohjelmissa on kymmeniä tai jopa satoja tuhansia komentoja.

Esimerkin vuoksi katsotaan, mitä ohjelmalle tapahtuu kun virus kiinnittyy siihen. Ensimmäinen oire viruksesta on tiedoston pituuden kasvaminen, joka 1701-viruksella on nimensä mukaisesti 1701 tavua. DIR-listaus kertoo uuden pituuden:

```
C>DIR CODE.COM

CODE     COM       1709 01.01.80    0.48
        1 tiedosto(a).Vapaana   11649024 tavua.
```

Kuten DIR-listaus osoittaa, ei tiedoston päivämäärä muutu vaikka virus kiinnittyykin siihen.

Kun uutta CODE.COM-ohjelmaa katsotaan DEBUGilla, nähdään miten virus on korvannut ohjelman ensimmäiset käskyt itseensä osoittavalla hypyllä. Joskus ohjelman alussa voi olla käskyjä, joita virus ei pysty muokkaamaan itselleen sopiviksi. Ohjelma voi olla myös liian pitkä, jotta hyppy ohjelman lopussa olevaan virusosuuteen onnistuisi. Tällaiset tiedostot ovat immuuneja, koska virus ei pysty tarttumaan niihin. Jos tartuntaa kuitenkin yritetään, lakkaa ohjelma toimimasta.

DEBUGin jälkeen annettava komento u 100 tarkoittaa, että konekielinen ohjelmakoodi halutaan muuntaa ihmisen luettavaksi assemblerkoodiksi (=unassemble) osoitteesta 100 alkaen, joka on ohjelman latausosoite muistissa. Assembler-listauksessa näkyvät muistisegmentti (esimerkissä 1986), siirros (offset), konekielikoodin numerot sekä numerot tulkittuna selväkielelle.

```
C>DEBUG CODE.COM
-u 100
1986:0100 E90600        JMP 0109
1986:0103 16            PUSH SS
1986:0104 B44C          MOV AH,4C
1986:0106 CD21          INT 21
1986:0108 01FA          ADD DX,DI
1986:010A 8BEC          MOV BP,SP
1986:010C E80000        CALL 010F
1986:010F 5B            POP BX
1986:0110 81EB3101      SUB BX,0131
1986:0114 2E            CS:
1986:0115 F6872A0101    TEST BYTE PTR [BX+012A],01
1986:011A 740F          JZ 012B
1986:011C 8DB74D01      LEA SI,[BX+014D]
```

Listaus näyttää, että alkuperäisen ohjelman kaksi viimeistä riviä ovat entisillä paikoillaan. Kun virus on saanut itsensä muistiin, se palaa takaisin suorittamaan alkuperäistä ohjelmaa.

Osoite, josta viruksen koodi alkaa, näyttää DEBUGilla katsottuna seuraavalta:

```
-u 0109
1986:0109 FA            CLI
1986:010A 8BEC          MOV BP,SP
1986:010C E80000        CALL 010F
1986:010F 5B            POP BX
1986:0110 81EB3101      SUB BX,0131
1986:0114 2E            CS:
1986:0115 F6872A0101    TEST BYTE PTR [BX+012A],01
1986:011A 740F          JZ 012B
1986:011C 8DB74D01      LEA SI,[BX+014D]
1986:0120 BC8206        MOV SP,0682
1986:0123 3134          XOR [SI],SI
1986:0125 3124          XOR [SI],SP
1986:0127 46            INC SI
1986:0128 4C            DEC SP
```

Valitettavasti 1701-viruksen sielunelämää ei voi seurata tämän pidemmälle pelkän DEBUG-ohjelman avulla. Etsintäohjelmien hämäämiseksi virus on koodattu niin, että sen komennot muuttuvat jatkossa käsittämättömäksi sotkuksi. Virus purkaa itsensä ajokuntoon vasta päästessään keskusmuistiin. Alkuperäisen ohjelman kaksi ensimmäistä komentoa on myös koodattu, joten niitäkään ei näy listauksessa.

Oikein tehdyn viruksen pitää välttää tarttumasta samaan tiedostoon monta kertaa. Viruksen on siksi tutkittava ohjelman alku tai loppu ennen tarttumistaan siihen. Vielä helpommalla virus pääsee tallentamalla hakemistoon merkin siitä, että tiedosto on jo käsitelty. Tiedostonimen lisäksi hakemistossa lukevat tiedoston määreet, tekoaika, päiväys, pituus ja osoitin FAT-taulukkoon. Merkkinä voi olla esimerkiksi vuosiluvun kasvattaminen sadalla. Koska DIR-listaus näyttää vuodesta vain kaksi viimeistä numeroa, ei vuosisata tulostu koskaan näkyviin. Myös kellonaikaa voi käyttää apuna. Se tallennetaan hakemistoon kahden sekunnin tarkkuudella, vaikkei DIR-komento näytä sekunteja lainkaan. Jos sekuntimäärä on yli 60, tietää virus ohjelman jo saaneen tartunnan.

Kirjoitussuoja ja lukumääre

DOSin mukana tulee kaksi tapaa säilyttää tiedostot koskemattomina. Ensimmäinen näistä on levykkeen kirjoitussuoja ja toinen lukumääre. Virustorjunnan kannalta ensimmäisestä on hyötyä, toisesta yleensä ei.

Levykkeen kirjoitussuoja asetetaan päälle eri tavoin riippuen siitä, onko kyseessä 5,25 tuuman lerppu vai 3,5 tuuman korppu. Lerpuilla tarvitaan pieni teippi, jolla peitetään levykkeen oikeassa yläreunassa oleva kolo. Koska kolon tunnistaminen tapahtuu optisesti, ei teippi saa olla läpinäkyvää! Korpuilla kirjoitussuoja otetaan käyttöön paljastamalla oikeassa ylänurkassa näkyvä tunnisteaukko. Toiminta on päinvastainen kuin lerpuilla: suoja on päällä, kun aukko näkyy ja pois päältä, kun aukon edessä on muoviläppä.

Korput ovat helpompia suojata, koska muoviläppä kulkee aina levykkeen mukana ja on helppo kytkeä päälle tai pois. Lerppujen mukana tulee arkillinen tarrateippejä, mutta teipit ovat yleensä hukassa silloin kun niitä tarvittaisiin. Teippiä on myös hankala poistaa kun levykkeelle halutaan jälleen kirjoittaa.

Levykkeen kirjoitussuojaan voi luottaa. Kun se on päällä, ei levykkeelle voi kirjoittaa eikä sitä voi alustaa. Suojausta ei ainakaan PC-koneissa voi ohittaa ohjelmallisin keinoin. Keskusmuistissa piileskelevä virus ei pysty kopioimaan itseään suojatulle levykkeelle eikä tarttumaan siltä käynnistettyihin ohjelmiin. Ikävä vain, ettei useimmissa kiintolevyissä ole samanlaista suojausmahdollisuutta.

Yrittäessään turhaan tarttua suojatulle levykkeelle virus saattaa pysähtyä "write protected error"-virheilmoitukseen. Kirjoitusyritykset tuottavat usein myös tavallisuudesta poikkeavia ääniä levykeasemasta ja levykkeen käyttö hidastuu selvästi. Nämä kaikki voivat johtaa viruksen paljastumiseen, jos käyttäjä osaa tulkita merkit oikein.

Kirjoitussuojan käyttö suojaa aina koko levyn. Yksittäisiä tiedostoja suojataan DOSin ATTRIB-apuohjelmalla. Ohjelma sekä asettaa että poistaa suojausmääreen (read-only). Kun määre on päällä, ei tiedostoa voida poistaa eikä sen sisältöä muuttaa. Tiedoston suojaaminen tapahtuu kirjoittamalla

```
C>ATTRIB +R COMMAND.COM
```

ja määreen poistaminen vastaavasti komennolla

```
C>ATTRIB -R COMMAND.COM
```

Ellei R-parametria anneta, tulostaa ohjelma tiedoston määreet. Jos suojausmääre on käytössä, tulostuu tiedostonimen eteen R-kirjain:

```
C>ATTRIB COMMAND.COM

A   R   COMMAND.COM
```

A-kirjain kertoo, että myös tiedoston arkistointimääre on päällä. Tiedostoa on siis muutettu viimeksi suoritetun varmistuksen jälkeen.

Mikronkäyttäjiä neuvotaan usein suojaamaan ATTRIB +R:llä päähakemiston tärkeät CONFIG.SYS-, AUTOEXEC.BAT- ja COMMAND.COM-tiedostot. Näin kannattaakin tehdä, sillä se estää muuttamasta niitä vahingossa tai kopioimasta levykkeeltä saman nimisiä tiedostoja alkuperäisten päälle. Suojausmääre tehoaa kuitenkin vain harvoja viruksia vastaan. Koska määre voidaan asettaa ohjelmallisesti, voidaan se myös poistaa samalla tavoin. Ennen kuin virus tarttuu ohjelmaan, se tarkistaa määreiden arvon ja jos suojausmääre on käytössä, se otetaan pois. Tarttumisen jälkeen mahdollinen määre asetetaan takaisin ilman, että käyttäjä huomaa mitään.

Tiedoston piilottamisesta ei liioin ole hyötyä. Laittamalla tiedoston piilomääre päälle voidaan tiedoston näkyminen DIR-listassa estää, mutta viruksen näkemiin tiedostoihin tämä ei vaikuta.

Mitä virus voi tehdä?

Tietokoneviruksiin heijastuvat monet arkisen elämän asiat. Yksi näistä on "pahanteon laki", joka näyttää vallitsevan kaikkialla. Laki määrää, että pahan tekeminen on aina helpompaa kuin hyvän tekeminen. Jos

ihminen haluaa tehdä pahaa, se todennäköisesti myös onnistuu. Paha on jopa helpompi määritellä kuin hyvä. Sen sijaan hyvätkin aikomukset ja sellaisiksi aiotut teot saattavat kääntyä päälaelleen tai toimia tarkoitustaan vastaan.

> Universaalinen laki numero 1:
>
> Pahan tekeminen on aina helpompaa kuin hyvän tekeminen.

Tietokoneissa laki toimii erityisen tehokkaasti, sillä ison ja lähes korjaamattoman vahingon tekeminen on helppoa. Tiedostot, joiden tekemiseen on käytetty satoja työtunteja, voidaan tuhota käyttökelvottomiksi muutamassa sekunnissa. Erilaisten vahinkojen tekemiseen on niin monta tapaa, että viruksen ainoaksi ongelmaksi jää valinnan vaikeus.

Levyn alustaminen

Usein kuvitellaan, että kiintolevyn alustaminen on pahinta mitä virus voi tehdä. Kaikki riippuu siitä, miten alustaminen tapahtuu. Jos kyseessä on looginen alustus, jollaisen mm. käyttöjärjestelmän FORMAT-ohjelma tekee, ei levyn tiedostoihin itse asiassa kosketa lainkaan. FORMAT-ohjelma käy ainoastaan nollaamassa FATin ja tyhjentämässä päähakemiston, jonka jälkeen levy näyttää tyhjältä. Tiedostot ovat kuitenkin edelleen levyllä ja niitä voi jopa yrittää palauttaa sopivilla apuohjelmilla (kuten Nortonin FR).

Low-level formatointi eli kiintolevyn perusalustus onkin jo vakavampi juttu. Siinä levy ja sen urat kirjoitetaan kokonaan uusiksi, yleensä täyteen nollaa. Tiedostojen palauttamista ei voi edes harkita.

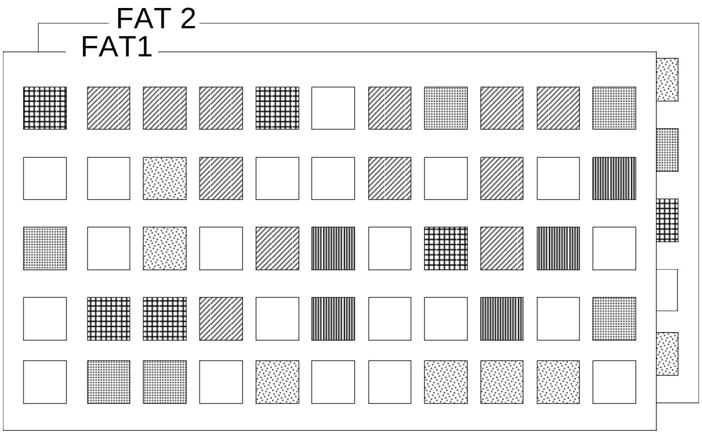
Levyn alustaminen vie aina runsaasti aikaa. Jos käyttäjä huomaa, että virus on aloittanut levyn alustamisen, ehtii sähköt katkaisemalla pelastaa vielä osan levystä. Erityisen helppoa tämä on FORMAT-ohjelman kohdalla. Aluksi FORMAT käy lukemassa levyn läpi tutkien,

onko sille syntynyt uusia vika-alueita. FAT ja päähakemisto tyhjennetään vasta viimeiseksi. Jos koneesta katkaistaan sähköt ennen kuin FORMAT-ohjelma on ehtinyt tähän vaiheeseen asti, huomataan ettei levyn tiedostoille ole tapahtunut mitään vahinkoa. Älä kuitenkaan kokeile asiaa omalla tärkeällä levylläsi!

FATin sotkeminen

Paljon kiintolevyn alustamista nopeampi keino vahingon tekemiseen on FATin sotkeminen tai sen kirjoittaminen täyteen nollaa. Koska FATin koko on levykkeillä muutamia kiloja ja kiintolevyllä muutamia kymmeniä kiloja, ei kirjoitus kestä kuin hetken - ja vahinko on taattu.

Jo ihan tavallisella 20 megatavun kiintolevyllä, jonka varausyksikön koko on 2 kilotavua, on 10000 FAT-alkiota. Jos nämä menevät sekaisin ja käyttäjä haluaa koota tiedostot takaisin kuntoon, hänellä on edessään 10000 palan palapeli - ilman kuvia.



Jos FATit sotketaan , osoittavat niiden alkiot minne sattuvat eikä levyltä voi enää hakea tiedostoja. Kuvassa olevan FATin pystyisi vielä järjestämään sopivan levytyökalun avulla, mutta kun kiintolevyn FATissa on kymmeniä tuhansia alkioita, on työ lähes toivotonta. Isot, yhtenäiset tiedostot voidaan etsiä levyltä esimerkiksi Nortonin avulla ja palauttaa levykkeelle, mutta pirstoutuneiden tiedostojen kokoaminen pala palalta on käytännössä mahdotonta.

Nollauran sotkeminen

Nollauran tyhjentäminen tai sen kirjoittaminen täyteen satunnaisia merkkejä tekee kiintolevyn hetkessä käyttökelvottomaksi. Koska osiotaulukko menetetään, ei DOS tunnista koko kiintolevyä eikä suostu siirtymään C: asemalle jotta levyn korjausta tai tiedostojen pelastamista voitaisiin edes yrittää. Kun tähän vielä yhdistetään FATin sotkeminen voidaan olla varma siitä, ettei levyltä pysty pelastamaan mitään. Ainoa mahdollisuus on luoda osiojako uudelleen FDISKillä ja alustaa tämän jälkeen koko levy.

Tiedostojen poistaminen

Poistetun tiedoston palauttaminen takaisin käyttöön on nykyisin niin helppoa, että harvat virukset edes vaivautuvat poistamaan levyllä olevia tiedostoja. Tarvitaan vain Nortonin tai PC-Toolsin kaltainen apuohjelma ja lähes mikä tahansa poistettu tiedosto saadaan takaisin käyttöön.

Oleellista on kuitenkin se, että palauttaminen tehdään heti poistamisen jälkeen. Mitä enemmän aikaa ehtii kulua poistamisen ja palautuksen välillä, sitä epätodennäköisemmäksi palautuksen onnistuminen muuttuu. Aikaa myöten käyttöjärjestelmän on otettava poistetut levyalueet uuteen käyttöön, jonka jälkeen tiedostoa ei voida palauttaa ainakaan kokonaisuudessaan.

Tunnetuin tiedostoja poistavista viruksista on Jerusalem. Perjantaina 13. päivä se poistaa jokaisen ohjelman, jota käyttäjä yrittää ajaa - myös sen palautusohjelman, jolla poistettuja tiedostoja yritetään palauttaa!

Tiedostojen sisällön muuttaminen

Edellä kuvatut temput ovat ilkeitä, mutta niissä on sentään yksi lohtu: tiedostot voidaan palauttaa takaisin käyttöön varmuuskopioilta. Pahimmillaan menetetään parin päivän työt, mutta ainakin käyttäjä oppii varmuuskopioinnin merkityksen.

Huomattavasti pelottavampia ovat virukset, jotka tuhoavat tiedostoja salakavalasti esimerkiksi kirjoittamalla niiden keskelle puppua. Ulospäin tiedostot näyttävät olevan täysin kunnossa. Niitä voi kopioida hakemistosta toiseen ja niistä voi hyvässä uskossa tehdä varmuuskopioita. Tiedostolle tapahtunut vahinko paljastuu vasta kun sitä yritetään käyttää. Jos kyseessä on ohjelmatiedosto, ohjelma ei käynnisty tai lukitsee koneen. Työtiedoston tapauksessa avaamista yrittävä ohjelma saattaa antaa virheilmoituksen tai jäädä jumiin. Tehdyistä varmuuskopioista ei ole mitään apua, koska nekin ovat vioittuneita.

Pilat

Ohjelmoijalla, joka haluaa pilailla uhrinsa kustannuksella, on monta eri mahdollisuutta. Helpointa on tulostaa kuvaruudulle erilaisia viestejä. Esimerkiksi 847-virus tulostaa tekstin

```
Program sick error.
Call doctor or buy PIXEL for cure description.
```

Harmittoman Sunnuntai-viruksen tekijä on selvästi kantanut huolta käyttäjän hyvinvoinnista. Virus aktivoituu nimensä mukaisesti sunnuntaisin ja tulostaa ruudulle kysymyksen "Today is sunday. Why do you work so hard?".

Yleinen 1701-virus aktivoituu puolestaan syksyllä ja pudottaa silloin ruudulla näkyvät kirjaimet näytön alariville putoavien lehtien tapaan. Italialainen virus lähettää kuvaruudulle pienen pomppivan pallon ja niin edelleen. Erilaisia osoituksia tekijöidensä huumorintajusta riittää.

Ylivoimaisesti kekseliäin on kuitenkin ollut Fu Manchu-viruksen tekijä. Virus seuraa näppäimistöä ja tarkkailee, mitä käyttäjä kirjoittaa. Aina, kun se huomaa sanat Thatcher, Reagan, Botha tai Waldheim, se lisää perään "is zzzz" missä zzzz on jokin ruma sana. Voi vain kuvitella, millaisen vaikutuksen tekee viruksen pilaama kirje, joka lähetetään jonkin maan hallituksesta virallisessa kirjekuoressa vaikkapa Yhdysvaltojen suurlähetystöön!

Virus voi myös sotkea kirjoittimelle menevän tulostuksen niin, että kirjaimet muuntuvat toisiksi joko täysin sattumanvaraisesti tai tiettyä kaavaa noudattaen. Erityisen kiusallinen vika on PostScript-kirjoitinta käytettäessä, koska PostScript tulostaa vain virheettömät sivut. Jos kirjoittimelle tulevassa PostScript-ohjelmakoodissa on virheitä, ei paperille tulostu mitään. PostScript-kirjoittimissa ei myöskään ole virheiden varalta merkkivaloja tai numerokoodeja, joista voisi päätellä mitä on tapahtunut. Kirjoittimen seotessa ei käyttäjä useinkaan tule edes ajatelleeksi viruksen mahdollisuutta.

Vaikka pilat onkin tarkoitettu humoristisiksi, ne voivat pahimmillaan olla hyvin kiusallisia, kuten eräs Atarista tavattu virus osoittaa. Oltuaan jonkin aikaa muistissa tämä virus alkaa matkia lämpöhäiriöitä tulostamalla kuvaruudulle satunnaisia merkkejä. Oireet viittaavat vialliseen muistipiiriin, joka alkaa sekoilla lämmetessään. Kone viedään huoltoon, mutta ahkerasta muistipiirien vaihtamisesta huolimatta sitä ei vain saada kuntoon.

Folklore

Tekniikan täsmällisestä luonteesta huolimatta ei ala ole välttynyt ihmisen tuomalta epätäsmällisyydeltä. Ihminen ei muutu, vaikka hänen työvälineensä muuttuisivatkin. Niinpä myös uskomukset, kaverilta toiselle kerrotut tarinat ja hurjat huhut elävät voimakkaina mikron käyttäjien keskuudessa ja kiertävät nopeasti.

Lukuisia ovat tarinat viruksista, jotka leviävät modeemin kantoaallolla, polttavat kuvaputkeen reiän, rikkovat kiintolevyjä tai kuormittavat mikropiirejä niin, että ne alkavat savuta. Yhtään tällaista virusta ei kuitenkaan ole saatu kiinni eikä pystytty tutkimaan. ATK-alan kansanperinne tuntuu siitä huolimatta elävän ja voivan hyvin.

3

Miten viruksesta pääsee eroon?

Kun käyttäjä huomaa, että omassa koneessa on virus, ovat hyvät neuvot tarpeen. Niitä annetaan tässä luvussa. Valitettavasti vain viruksia on niin monenlaisia, ettei mitään ehdotonta työjärjestystä tai ohjekirjaa voida antaa. Viruksen lopullinen tuhoaminen riippuu paljolti siitä, millainen virus on kyseessä. Tapoja viruksen tunnistamiseen on esitelty lähemmin ensimmäisessä liitteessä.

Toimintajärjestys

Varman virushavainnon jälkeen on ensimmäinen tehtävä katkaista koneesta sähkö. Katkaiseminen pitää suorittaa virtakytkimestä, sillä virukset saattavat selvitä CTRL-ALT-DEL -käynnistyksestä. Vasta sitten aletaan kaikessa rauhassa miettiä, mitä oikein kannattaisi tehdä. Turha hosuminen johti Englannissa väärän suihkumoottorin sammuttamiseen ja matkustajakoneen putoamiseen hieman ennen kiitoradan alkua. Samaa virhettä ei kannata tehdä mikronsa kanssa. Niin kauan kuin ei tee mitään, ei voi myöskään tehdä virheitä.

Ennen kuin virusta aletaan poistaa, on levylle jääneet työtiedostot pelastettava. Virus olisi myös yritettävä tunnistaa, koska tieto siitä, mikä virus on kyseessä, voi merkittävästi vähentää viruksen tuhoamiseen vaadittavaa työtä. Varmuuden vuoksi voi tietenkin tyhjentää koko kiintolevyn ja alustaa sen uudelleen, mutta vaarattomien virusten

Kun virus havaitaan...

1. Tunnistaminen

2. Varmuuskopiointi

3. Puhdistaminen

4. Tiedostojen palauttaminen

5. Jälkihoito

Muista:
- harkitse ennen kuin toimit
- varoita muita

kohdalla pelkkä saastuneiden tiedostojen poistaminenkin saattaisi riittää. Tapoja viruksen tunnistamiseen on käsitelty ensimmäisessä liitteessä. Jos kyseessä on esimerkiksi ohjelmiin tarttuva virus, on se helppo tunnistaa pituudesta, jolla ohjelmat ovat kasvaneet.

Jotta tiedostoja voitaisiin varmistaa ja viruksen tunnistamista yrittää, on kone käynnistettävä uudelleen. Käynnistys on tehtävä alkuperäisellä DOS-levykkeellä tai sen puhtaaksi tiedetyltä kopiolta. Levykkeellä pitää ehdottomasti käyttää kirjoitussuojaa! Muutoin koneessa pesivä virus saattaa tarttua myös uudelle levykkeelle.

Kun mikro on jälleen saatu käyntiin, on tärkeätä, ettei mitään kiintolevyllä olevaa ohjelmaa käynnistetä edes vahingossa. Ohjelmatiedostoihin tarttunut virus pääsee käynnistyksessä muistiin ja tekee varmistuksen turhaksi. Kaikki ohjelmat on siis käynnistettävä puhtaaksi tiedetyltä A: levykkeeltä. Hakureitti PATH kannattaa varmuuden vuoksi asettaa osoittamaan A: levykettä, jottei ohjelmia edes vahingossa haeta kiintolevyltä. Koska DIR- ja COPY-komennot eivät ole apuohjelmia vaan kuuluvat käyttöjärjestelmän komentotulkkiin (COMMAND.

COM, joka on ladattu puhtaalta A: levykkeeltä), voidaan niitä käyttää normaaliin tapaan.

Tiedostojen varmistaminen

Vaikka käyttäjä olisi hoitanut varmuuskopioinnin säännöllisesti, eivät varmistukset koskaan ole täysin ajan tasalla. Ensimmäinen tehtävä onkin varmistaa kiintolevyllä olevista työtiedostoista tärkeimmät. Ohjelmatiedostoja ei pidä kopioida, sillä virus voi olla kiinnittynyt mihin ohjelmaan tahansa. Jos jokin kiintolevyllä olevista ohjelmista on erityisen tärkeä eikä siitä ole varmuuskopiota, voi ohjelman kopioida erilliselle levykkeelle. Kiintolevyn puhdistuksen jälkeen ohjelma palautetaan takaisin kiintolevylle vain jos sen puhtaus saadaan varmistettua tai ohjelmassa oleva virus poistettua jonkin luvussa seitsemän kuvatun apuohjelman avulla.

Työtiedostojen kopiointi levykkeille kannattaa tehdä tavallisella COPY-käskyllä. BACKUPia tai XCOPYä ei kannata käyttää, koska ne pitäisi ladata puhtaalta DOS-levykkeeltä eikä niiden toimintaperiaatekaan sovi yksittäisten työtiedostojen kopiointiin.

Kun äkillinen tarve varmuuskopiointiin yllättää, ei ulottuvilla useinkaan ole valmiiksi alustettuja levykkeitä. Tällöin on tärkeätä, ettei varmistuksia tehdä vanhojen varmistusten päälle. Eräät virukset nimittäin tuhoavat tiedostoja salakavalasti ja tuho paljastuu vasta kun tiedostoja yritetään käyttää. Pilaantuneiden tiedostojen kopiointi vanhojen, kunnossa olevien varmistusten päälle vain pahentaa tilannetta. Varmistukset on siksi tehtävä tyhjille tai tarpeettomiksi käyneille levykkeille. Ellei tällaisia ole ulottuvilla, on niitä alustettava. FORMAT-ohjelma pitää nytkin ladata alkuperäiseltä DOS-levykkeeltä eikä kiintolevyllä olevaa FORMAT-ohjelmaa pidä käyttää.

Viruksen tunnistaminen

Kun tiedostot on varmistettu, voidaan yrittää viruksen tunnistamista. Tunnistamista kannattaa yrittää, sillä eräistä viruksista pääsee eroon

suhteellisen helposti. Tunnistus voi onnistua tässä kirjassa olevien viruskuvausten avulla. Tuntomerkkeinä voivat olla esimerkiksi koko, jolla saastuneet tiedostot kasvavat tai käynnistyslohkosta löytyvät koodit. Varminta on kuitenkin käyttää jotain luvussa seitsemän esiteltyä virusten etsintäohjelmaa.

Koska uusia viruksia kehitetään koko ajan, ei mikään etsintäohjelma voi tuntea niitä kaikkia. Lisäksi eräät virukset (kuten Brain ja 666) osaavat huijata etsintäohjelmia siten, etteivät nämä löydä virusta järjestelmästä. Etsintäohjelmat eivät siksi voi koskaan antaa täyttä varmuutta viruksesta.

Kiintolevyn puhdistaminen

Mikäli mikrosta löytynyt virus on tiedostoon tarttuvaa tyyppiä, pääsee viruksesta eroon poistamalla saastuneet tiedostot. Tällaisia helposti nujerrettavia viruksia ovat mm. Jerusalem B, Vacsina, Yankee Doodle ja 1701. Ellei käytettävissä ole virusten paljastusohjelmaa, joka kertoisi saastuneiden tiedostojen nimet, on syytä poistaa levyltä kaikki ohjelmatiedostot ja palauttaa ne takaisin alkuperäisiltä ohjelmalevykkeiltä. Aiemmin tehtyjä varmuuskopioita ei pidä käyttää, koska niiden puhtaudesta ei voida olla varmoja.

Kaikki tiedostoviruksetkaan eivät ole näin helppoja tapauksia. Esimerkiksi tiedostoihin kiinnittyvä Dark Avenger sotkee kaikessa hiljaisuudessa levyn tiedostoja niin, ettei niitä voi enää käyttää. Tällöin on edessä koko levyn puhdistaminen eikä edes kaikkia kiintolevyllä olevia työtiedostoja voi käyttää.

Käynnistyslohkoon kiinnittyvästä viruksesta pääsee eroon SYS-ohjelmalla. Komento

```
A>SYS C:
```

kopioi A: asemassa olevat käyttöjärjestelmätiedostot C: asemaan, vanhan käyttöjärjestelmän päälle. Samalla se kirjoittaa myös C: levyn käynnistyslohkon uudelleen, mikä yleensä riittää tuhoamaan lohkossa piileskelleen viruksen. Alkuperäisen käynnistyslohkon kopio jää

kuitenkin levylle - usein bad sectoriin tai nollauralle kopioituna. Koska virus on tapettu, ei ylimääräinen kopio tuota varsinaista haittaa. Korkeintaan se saattaa antaa vääriä hälyytyksiä eräitä virusten etsintäohjelmia käytettäessä.

Osiotaulukkoon kiinnittyneestä viruksesta (mm. Stoned) on kaikkein hankalinta päästä eroon, sillä edes kiintolevyn alustaminen FORMAT-ohjelmalla ei tyhjennä osiotaulukkoa. Taulukon puhdistamista voi yrittää Nortonin tai PC-Toolsin kaltaisilla apuohjelmilla, mutta helpoiten se käy virusten poistamiseen tarkoitetulla apuohjelmalla (kuten McAfeen CLEAN).

Jos virus on tuhonnut nollauran, on myös osiotaulukko sekaisin eikä DOS salli edes C: asemalle siirtymistä. Vain levykeasemia A: ja B: voidaan käyttää. Jos yritetään siirtyä C: asemalle, saadaan pahaenteinen virheilmoitus

```
A>C:
Invalid drive specification
```

Levyasema ei ole rikki, vaikka virheilmoituksesta voisi saada sen käsityksen. Tässä tapauksessa levyn osiotaulukko on rakennettava uudelleen FDISK-ohjelmaa käyttäen ennen kuin tiedostojen palauttamista voidaan edes yrittää.

Varminta alustaa kiintolevy uudelleen

Olipa virus mitä tyyppiä tahansa, siitä pääsee varmimmin eroon tyhjentämällä koko kiintolevyn. Näin on syytä tehdä aina, kun viruksen tyypistä tai toimintatavoista ei olla täysin varmoja.

Levyn alustaminen pelkällä FORMAT-ohjelmalla ei vielä riitä, koska FORMAT ei kirjoita levyä täyteen nollaa eikä fyysisesti poista tiedostoja. Alustaminen pitäisikin tehdä ns. perusalustuksena, low level formatointina. Tätä varten useimpien mikrojen mukana toimitetaan INITHD- tai HDINIT-niminen ohjelma. Alustus voi myös löytyä mukana tulleen SETUP-ohjelman valikosta. Koska ohjelmat ovat valmistajan omaa tekoa eivätkä tule käyttöjärjestelmän tekijältä (Mic-

Kiintolevyn täyspuhdistus

1. Low-level formatointi (HDFORMAT, INITHD tms.)

2. Osioiden perustaminen (FDISK)

3. Ensiöosion alustaminen (FORMAT C: /S /V)

4. Muiden osioiden alustaminen (FORMAT D:/V, E:/V jne)

5. DOS-hakemiston luominen C:lle

6. Ohjelmatiedostojen palauttaminen

7. Työtiedostojen palauttaminen

rosoft tai IBM), ne sijaitsevat normaalisti diagnostiikka- tai apuohjelmalevykkeellä. Alkuperäiseltä DOS-levykkeeltä niitä on turha etsiä.

Perusalustaminen kestää paljon tavallista FORMAT-ohjelmaa kauemmin. Isoilla levyillä aikaa saattaa kulua jopa useita tunteja. Työn aikana koko kiintolevy kirjoitetaan täyteen nollaa ja myös sillä olevat magneettiurat ja ohjausmerkit kirjoitetaan uudelleen. Alustuksen jälkeen levy pitää jakaa osioihin (FDISK), osiot alustaa FORMATilla, käyttöjärjestelmä siirtää C:lle ja luoda hakemistorakenne. Näitä asioita on käsitelty tarkemmin Uudessa PC-käyttäjän käsikirjassa.

Levykkeillä FORMAT-ohjelma suorittaa aina perusalustuksen. Levykkeen alustaminen tuhoaa totaalisesti sen aiemman sisällön, joten myös mahdolliset virukset poistuvat. Jos alkuperäinen FORMAT-ohjelma on korvattu jollakin apuohjelmalla (esimerkiksi PC-Toolsin mukana tulevalla PCFORMAT-ohjelmalla), saattavat myös levykkeen tiedot säilyä alustamisen yli.

Kun kiintolevy on saatu puhdistettua, palautetaan sille ohjelmat ja työtiedostot. Kaikki ohjelmat on palautettava alkuperäisiltä toimituslevykkeiltä eikä mitään kopioita pidä käyttää. Ohjelmien asentamisessa

takaisin kiintolevylle on melkoinen työ, mikä saattaa houkutella aiemmin tehtyjen varmuuskopioiden käyttöön. Asentamisessa kannattaa kuitenkin olla perusteellinen, sillä jos virus pääsee livahtamaan takaisin mikroon jonkin kopioidun ohjelman mukana joudutaan koko puhdistusoperaatio suorittamaan uudestaan.

Levykkeiden jäljittäminen

Kun oma kiintolevy on saatu jälleen toimintakuntoon, alkaa kaikkein työläin vaihe: pitää jäljittää kaikki ne levykkeet, joille virus on voinut kopioida itsensä. Omat levykkeet on yleensä käyty nopeasti läpi, mutta useimmat käyttäjät vaihtelevat levykkeitä myös muiden käyttäjien kanssa ja vievät joskus levykkeitä kotoa töihinkin.

Levykkeeltä, jonka epäillään saaneen virustartunnan, ei nytkään pidä ajaa yhtään ohjelmaa - ei edes vahingossa. Vahinko sattuu helposti, mikäli käytetään esimerkiksi CHKDSK-ohjelmaa joka sattuu löytymään myös levykkeeltä. Jos oletuslevyasema on komennon antamishetkellä A:, latautuu ohjelma viruksen saastuttamalta levykkeeltä. Yksi tällainen erehdys riittää, jotta virus pääsee takaisin kiintolevylle.

Virusten luotettava etsiminen levykkeiltä ilman kunnon apuohjelmia on lähes mahdotonta, eikä kaikkia levykkeitä voi suin päin alustaa uudelleen. Virusten etsintäohjelmat ovatkin kullanarvoisia saastuneita levykkeitä jäljitettäessä.

Kun omat levykkeet on käyty läpi, on tuttavien vuoro. Kenelle annoitkaan viimeksi levykkeitä? Anna heille nyt myös virusten etsintäohjelma ja kerro, mitä kohdallesi on sattunut. Näin voit estää vahinkoa leviämästä. Virustartunnasta kertominen on käyttäjien keskinäistä solidaarisuutta. Koskaan ei voi tietää, milloin sellainen sattuu omalle kohdalle.

Virus yrityksessä

Mikäli virus löytyy omasta kotimikrosta, on sen puhdistaminen edellä kuvatulla menettelyllä vielä suhteellisen helppoa. Yrityksissä, kouluis-

sa ja muissa vastaavissa yhteisöissä tilanne on paljon hankalampi. Koska levykkeitä vaihdellaan koneesta toiseen, pääsee virus leviämään helposti. Jos mikroja on useita kymmeniä, on niiden kaikkien läpikäynti ja puhdistaminen todellinen tukihenkilön painajainen. Sen rinnalla Wordperfectin vaihtaminen uuteen versioon on vielä lasten leikkiä. Tukihenkilön kannattaa mieluummin torjua virukset jo ennakolta, jotta kuvatunkaltaista tilannetta ei pääse syntymään.

Lähiverkko auttaa virusten leviämistä. Vaikka virus ei suorastaan leviäkään verkon läpi, riittää esimerkiksi palveluasemassa sijaitseva saastunut ohjelmatiedosto levittämään viruksen jokaiseen työasemaan.

Koska viruksesta on näin työlästä päästä eroon, on helpointa keskittyä ennaltaehkäisyyn. Seuraava luku käsitteleekin tapoja, joilla voi vähentää virustartunnan mahdollisuuksia.

4

Varautuminen viruksia vastaan

Jos viruksen on kerran saanut, on siitä pahimmassa tapauksessa hyvinkin vaikeata päästä eroon. Paras tapa torjua viruksia on siksi ennaltaehkäisy. Yksinkertaisia ohjeita noudattamalla voi merkittävästi vähentää viruksen saamisen todennäköisyyttä. Erityisen tärkeitä tällaiset ohjeet ovat yrityksissä. Tällöin tulee myös varmistaa, että ohjeita todella noudatetaan.

Viruksia torjuttaessa on tärkeätä, että yrityksen mikrokäyttäjiä motivoidaan tarpeeksi. Jos pelien pelaaminen ja ohjelmien kopiointi kielletään perustelematta asiaa sen kummemmin, ei kieltoakaan jakseta noudattaa. Kieltojen ja määräysten sijaan käyttäjille pitäisi kertoa siitä, mitä virukset ovat, mitä ne voivat saada aikaan ja miten viruksilta voidaan välttyä. Jokaiselle pitäisi tehdä selväksi, että ohjeiden laiminlyönnistä johtuva virustartunta saattaa aiheuttaa yritykselle ja sen käyttäjille suuret vahingot.

Kurinpalautus ja pelien pelaamiskielto ei kuitenkaan saa olla niin ehdoton, etteivät käyttäjät uskalla ilmoittaa tekemistään virushavainnoista.

Torjunnan kolme osa-aluetta

Virusten torjuntastrategiaan kuuluu kolme osa-aluetta:

- Virusten välttäminen
- Mahdollisen virustartunnan tunnistaminen riittävän ajoissa
- Selustan turvaaminen (varmuuskopiointi)

Mikään alueista ei yksinään riitä suojaamaan käyttäjää. Tehokas suoja syntyy vasta kun kaikkia kolmea menetelmää sovelletaan yhtä aikaa.

Seuraavassa tarkastellaan lähemmin kutakin osa-aluetta.

Virusten välttäminen

Ensimmäinen vaihe on virustartunnan välttäminen. Muutamaa selkeätä ohjetta noudattamalla voi merkittävästi vähentää todennäköisyyttä altistua virustartunnalle.

Älä kopioi ohjelmia toisilta

Virukset leviävät parhaiten kopioitujen ohjelmien välityksellä. Varsinkin kädestä käteen kiertävät peliohjelmat, joiden alkuperää ei oikein kukaan tunnu tietävän, ovat oivallinen tapa virusten levittämiseen. Pelien pelaamista mikrolla ei voi kieltää, mutta pelit kannattaa hankkia viralliselta myyjältä tai vaikka suoraan ulkomailta tilaamalla, jos se tulee halvemmaksi. Aiemmin PC-koneille tarkoitettujen pelien myyjiä ja maahantuojia oli vaikeata löytää, mutta tilanne on muuttunut. Jos muutaman satasen käyttäminen peliin tuntuu kalliilta ajattele, mikä on mahdollisen viruksen aiheuttaman vahingon hinta.

Kursseilla, joita olen pitänyt viruksista ja niihin liittyvistä asioista, olen joskus pyytänyt kaikkia suosittua ja tuhmaa Larry-peliä pelanneita nostamaan kätensä. Yleensä kätensä on nostanut n. 50-75% kuulijoista. Tämän jälkeen olen pyytänyt kaikkia niitä, jotka ovat ostaneet pelinsä, nostamaan kätensä. Toistaiseksi olen löytänyt Suomesta vain yhden pelinsä ostaneen henkilön. Kaikki muut - ja heitä on satoja - ovat käyttäneet pelin laittomasti kopioitua versiota. Näin siitä huolimatta, että

pelin hinta suomalaisella maahantuojalla on vain 350 markkaa. Enää ei kannata ihmetellä miksi virukset leviävät!

Älä tuo ohjelmalevykkeitä kotoa töihin

Mikrojen nopea yleistyminen on johtanut tilanteeseen, jossa monilla käyttäjillä on jo kaksikin mikroa, toinen työssä ja toinen kotona. Työpaikan mikrolla tehdään töitä ja usein niitä viedään vielä kotiinkin. Lapsia on mahdotonta estää vaihtelemasta pelejä kaverien kanssa ja ajamasta niitä kotikoneessa vanhempien ollessa poissa. Kun tällaisessa koneessa ajetaan sitten sovellusohjelmaa, joka levykkeen mukana siirretään takaisin työpaikan koneeseen, on olemassa selvä virustartunnan vaara.

Edes pelkkien työtiedostojen siirtäminen ei ole täysin turvallista. Käynnistyslohkoon piiloutuva virus saattaa levitä pelkkiä työtiedostoja sisältävällä levykkeellä. Jos koneessa on jokin sovellusohjelmavirus, se voi levitä sovelluksella tehdyn työtiedoston mukana. Lisäksi eräät tavalliset virukset sotkevat levyä kirjoittamalla olemassa olevien tiedostojen päälle. Jos käyttäjä siirtää tällaisen vioittuneen työtiedoston koneesta toiseen ja kopioi sen kiintolevylle, menetetään levyllä ollut saman tiedoston vanhempi, mutta kunnossa ollut versio. Macissä rajanveto ohjelma- ja työtiedoston välillä on joskus vaikeata joten työtiedostotkin saattavat sisältää viruksia. Riski vahingon tapahtumiseen työtiedostoja siirtämällä on kuitenkin hyvin vähäinen, eikä kotona työskentelyä kannata tästä syystä rajoittaa.

Älä käynnistä konetta tuntemattomalla levykkeellä

Jos koneessa on kiintolevy, sitä ei koskaan pitäisi käynnistää levykkeellä. Jos levykekäynnistystä välttämättä tarvitaan, on käynnistys tehtävä aina samalla kirjoitussuojatulla järjestelmälevykkeellä. Käynnistyslohkoon sijoittuvat virukset pääsevät muistiin vain kun kone käynnistetään tai käynnistystä edes yritetään saastuneella levykkeellä. Älä koskaan jätä levykettä A: asemaan kun lopetat mikron käytön, koska muutoin seuraava alkulataus tapahtuu tältä levykkeeltä.

Tarkista purkeista imuroimasi ohjelmat ennen käyttöä

Tietokoneharrastajien ylläpitämät purkit ("boxit") ovat todellisia mikroharrastajan aarreaittoja. Isoissa purkeissa on tarjolla tuhansia hyödyllisiä ohjelmia ja paljon asiantuntevaa tietoa. Kuka tahansa modeemilla ja tietoliikenneohjelmalla varustautunut harrastaja pystyy siirtämään ohjelmia purkista omaan mikroonsa ja päinvastoin. Tiedostojen siirtämistä purkista omaan koneeseen kutsutaan tuttavallisesti imuroinniksi (download).

Purkeista löytyviä ohjelmia ja asiantuntemusta kannattaa ehdottomasti käyttää hyväksi. Esimerkiksi uusimman virusten etsintäohjelman imurointi purkista kestää vain muutaman minuutin.

Purkit ovat saaneet hieman huonon maineen kun on arveltu, että virukset leviäisivät niiden jakamien ohjelmatiedostojen mukana. Tällainen pelko on useimmiten turhaa. Purkkien vastuuhenkilöt (system operator, "sysop") ovat yleensä hyvin tietoisia viruksista. Heillä on käytössään useita virusten etsintäohjelmia ja jos sysop seuraa tietoverkoissa kiertävää maailmanlaajuista viruskeskustelua, hän on erittäin hyvin perillä alan uusimmastakin kehityksestä.

Lähes jokaisessa purkissa on kuitenkin alue, johon kuka tahansa käyttäjä pystyy lähettämään ohjelmia ja tiedostoja ("upload area"). Sysop ei ole vastuussa tämän alueen ohjelmista eikä ole tarkistanut niiden puhtautta. Kannattaa siis välttää ohjelmien imuroimista tältä alueelta.

Uskaltaako purkeista imuroituja ohjelmia sitten käyttää? Kyllä varmasti. Ainoat, joita kannattaa varoa, ovat kiintolevyn käytön apuohjelmat, eikä niitäkään virusten vaan ohjelmavirheiden vuoksi. Purkkien ohjelmat ovat harrastajien tekemiä, eikä kukaan ota vastuuta niiden oikeellisuudesta. Koska kaupallisistakin ohjelmista löytyy virheitä, löytyy niitä varmasti myös purkkien ohjelmista. Mahdolliset virheet eivät yleensä estä ohjelman käyttöä, mutta saattavat eräissä tiedosto-ohjelmissa olla muuten tuhoisia. Enpä esimerkiksi itse suostuisi käyttämään julkisohjelmana levitettävää hakemiston aakkosjärjestysohjelmaa. Siinä yksikin virhe riittäisi sotkemaan levyn kirjanpidon. Muilta

purkin käyttäjiltä kannattaa kysyä, mitä ohjelmia he ovat käyttäneet ja mitä he suosittelevat.

Tarkista kaikki uudet levykkeet ennen käyttöä

Luvussa seitsemän esitellään ohjelmia, jotka tarkastavat levyn ja antavat varoituksen viruksen havaitessaan. Kaikki taloon tulevat levykkeet pitäisi tarkastaa ennen käyttöönottoa. Erityisesti tämä koskee ulkomailta ja varsinkin Itä-Euroopasta tulevia levykkeitä, vaikka ne olisivat alkuperäisiä ohjelmalevykkeitäkin. Esimerkiksi vaarallinen 4096-virus tuli Suomeen Israelissa tehdyn valmisohjelman levykkeellä.

Testaa epäilyttävät ohjelmat erillisessä koneessa

Mikään etsintä- tai torjuntaohjelma ei voi antaa suojaa kaikkia viruksia eikä varsinkaan troijalaisia vastaan. Jos on erityistä syytä epäillä ohjelman toimivuutta tai jos ohjelmalta muutoin vaaditaan ehdotonta virheettömyyttä esimerkiksi ennen sen asentamista lähiverkon palveluasemaan, jää ainoaksi mahdollisuudeksi asettaa ohjelma joksikin aikaa karanteeniin. Ohjelma asennetaan tarkoitusta varten hankittuun koneeseen, jota ei ole liitetty verkkoon ja jota ei käytetä mihinkään muuhun. Jotta lopputulos olisi luotettava, pitäisi ohjelmaa kokeilla monissa eri tilanteissa, esimerkiksi asettamalla koneen päiväys 13 päiväksi ja perjantaiksi, siirtämällä päiväystä vuodella eteenpäin, käyttämällä ohjelmaa useita vuorokausia yhteen menoon ja seuraamalla vika-alueiden määrässä, ohjelmien pituuksissa ja muissa vastaavissa tapahtuvia muutoksia. Vasta kun ohjelmaa on testattu riittävän pitkään eikä ongelmia ole havaittu, voidaan ohjelma ottaa yleiseen käyttöön.

Virustartunnan havaitseminen

Koska kaikki virukset ovat erilaisia, ei yksiselitteisiä ohjeita virusten havaitsemiseksi voi antaa. Seuraavassa on lueteltu joukko tapahtumia, jotka ovat tyypillisiä virusten aiheuttamia oireita. Kunkin oireen

kohdalla on pyritty listaamaan myös muita kuin viruksista johtuvia syitä syitä. Joka tapauksessa asia kannattaa tutkia. Jos yrityksessä on mikrotukihenkilö, hänet tulee kutsua paikalle. Mitä varhaisemmassa vaiheessa virus havaitaan, sitä vähäisemmäksi sen aiheuttamat vahingot jäävät.

Bad sectorien määrä kasvaa

Kun FORMAT-ohjelma alustaa levyn, se kirjoittaa levyllä olevien vika-alueiden (bad sector) osoitteet FAT-kirjanpitoon, jonka jälkeen DOS osaa kiertää ne. Vika-alueiden määrä ei normaalikäytössä lisäänny. CHKDSK-ohjelma ilmoittaa FATiin merkittyjen vika-alueiden määrän, mutta ei koskaan muuta tätä lukemaa - ei edes /F-valitsinta käytettäessä. Ainoat DOSin apuohjelmat, jotka voivat kasvattaa vika-alueiden määrää, ovat FORMAT ja RECOVER.

Levykettä, jolla on bad sectoreita, ei pitäisi koskaan käyttää. Jos vika-alueet ovat syntyneet alustamisen yhteydessä, ne ovat merkki levykkeen huonosta laadusta. Tällaisen levykkeen käyttäminen on ikävyyksien kerjäämistä. Toinen mahdollisuus on, että virus on luonut vika-alueet piilokseen. Vika-alueiden määrä on helppo tarkistaa CHKDSK-ohjelmalla.

Jos vika-alueiden määrä käytön aikana kasvaa, voi asialla olla virus joka yrittää piiloutua vialliseksi merkitsemäänsä kohtaan levyä. Vika-alueiden määrää voidaan muuttaa myös eräillä apuohjelmilla (mm. Nortonin DT, PC-Tools, Savedir ja Disk Technician, joista viimemainittu luo levylle ison vika-alueen lukupäiden pysäköintiä varten).

Ohjelmatiedostojen pituudet muuttuvat

Kun virus tarttuu ohjelmatiedostoon, tiedoston pituus kasvaa. Eräät virukset muuttavat myös tiedoston päiväystä. Ohjelmatiedoston pituuden kasvaminen on lähes varma merkki viruksesta, sillä käyttöjärjestelmässä ei ole mitään muuta tilannetta, jossa ohjelman pituus muuttuisi. Ohjelmatiedostot tuntee siitä, että niiden tunniste on .COM tai .EXE.

Eräät virukset tarttuvat myös ohjelmien käyttämiin kerrostustiedostoihin, joiden tunniste on .OVL.

Periaatteessa viruksen voisi havaita pitämällä kirjaa ohjelmatiedostojen pituuksista ja vertaamalla todellisia pituuksia aika ajoin tähän kirjanpitoon. Koska levyllä on normaalisti kymmeniä ohjelmia ja nekin eri hakemistoissa, ei työ olisi helppoa. Kannattaa kuitenkin seurata ainakin komentotulkin COMMAND.COMin pituutta. Se löytyy yleensä C: aseman päähakemistosta ja on monen viruksen mielikohde. Siihen tarttunut virus pääsee ajettavaksi keskusmuistiin jo koneen käynnistymisen aikana. Toisaalta paikka on niin ilmeinen, että eräät virukset välttävät sitä juuri samasta syystä. Unohtaa ei sovi myöskään KEYB-näppäinohjainta, joka on ensimmäinen COMMAND.COMin jälkeen ajettava ohjelma. Jos virus löytyy COMMAND.COMista, on se yleensä levinnyt myös KEYB.COMiin.

Jos haluaa tarkkailla tiedostojen pituuksia, kannattaa seurata yleisesti käytettyjä apuohjelmia kuten CHKDSK ja FORMAT. Myös yleisimmät sovellusohjelmat kannattaa ottaa seurantaan. Luvun lopussa on esitetty komentojonoja, joilla seuranta voidaan automatisoida.

PIF on tunniste, jolla merkitään ohjelmankuvaustiedostoja. Tiedosto kertoo, miten merkkipohjaisen DOS-sovelluksen pitää käyttäytyä Windowsin kanssa: mikä on ohjelmatiedoston nimi ja mistä hakemistosta se löytyy, paljonko ohjelma vaatii muistia, kirjoittaako se suoraan kuvaruutumuistiin ja niin edelleen. Esimerkiksi WP:n toimintaa kuvaava PIF-tiedosto on nimeltään WP.PIF. Vaikka PIF-tiedostot eivät olekaan ohjelmia, niitä käytetään joissain tapauksissa ohjelmien tavoin ja viruksetkin voivat tarttua niihin. Tartunnat on helppo huomata, sillä PIF-tiedostojen pituus on aina vakio. Vanhemmissa PIF-versioissa pituus oli 369 tavua. Uudemmissa, Windows 3:n PIF-tiedostoissa pituus on kasvanut 545 tavuun. Kaikki näistä poikkeavat arvot ovat merkkejä viruksista.

Windows lakkaa toimimasta

Windows on hyvä koekaniini erilaisille viruksille. Kun Windows ladataan muistiin ja käynnistetään, yrittävät virukset tarttua siihen.

Windowsin ja Windows-sovellusten käyttämän ohjelmatiedoston rakenne poikkeaa kuitenkin tavallisten DOS-sovellusten käyttämästä, eivätkä kaikki virukset tästä syystä onnistu tarttumisyrityksessään. Windows jää joko jumiin tai käyttäytyy muutoin oudosti.

Keskusmuistin määrä on pienentynyt

Koneessa olevan perusmuistin määrä ja siitä vapaana oleva osa nähdään CHKDSK-apuohjelman avulla. Jos virus haluaa majailla keskusmuistissa ja suojata itsensä poispyyhkimiseltä, on sen varattava osa muistista pysyvästi itselleen. Muistin väheneminen näkyy heti CHKDSKiä käyttämällä.

Perusmuistin määrää vähentävät myös monet CONFIG.SYS-tiedostoon tehtävät toiminta-asetukset sekä muistinvaraiset apuohjelmat, joita tulee DOSin omienkin apuohjelmien mukana. Jos esimerkiksi vertaa vapaan muistin suuruutta ennen ja jälkeen APPEND-, GRAPHICS- tai PRINT-ohjelmien käytön voi havaita, että muisti vähenee kun ohjelmaa käytetään ensimmäistä kertaa. Tämä johtuu siitä, että osa ohjelmasta jää pysyvästi muistiin eikä poistu sieltä vaikka ohjelman käyttö loppuukin. Vapaa muisti palautuu entiselleen vasta kun mikro sammutetaan ja käynnistetään uudelleen.

Tiedostoja katoaa ilman näkyvää syytä

Tiedostoja poistavista viruksista tunnetuin on Jerusalem B, joka poistaa kaikki ohjelmat, joita käyttäjä yrittää ajaa 13. päivä perjantaina. Monet muutkin virukset poistavat tiedostoja.

Tätä virusoiretta ei pidä kertoa aloittelevalle mikron käyttäjälle. Muutoin hän kutsuu tukihenkilöä paikalle jatkuvasti ja kertoo koneessaan olevan tiedostoja syövän viruksen. Olen itse huomannut, että salaperäisesti kadonneiden tiedostojen määrä on kääntäen verrannollinen mikron käyttökokemukseen. Mitä paremmin mikronsa oppii tuntemaan, sitä harvemmin tiedostoja näyttää katoavan. Käyttöjärjestelmän nykyversioissa ei enää ole virheitä, jotka johtaisivat tiedostojen katoamiseen.

Ohjelmat lakkaavat toimimasta

Viruksen saastuttama tiedosto voi lakata toimimasta monesta syystä. Eräs mahdollisuus on, ettei virus ole onnistunut tarttumaan ohjelmaan kunnolla. Kaikki virukset eivät ole kovin tarkkoja siitä, mihin itseään tai alkuperäisen boot-lohkon kopioivat. Jos kopiointi suoritetaan sellaiseen kohtaan levyä, jossa on jo jokin työ- tai ohjelmatiedosto, muuttuu tiedosto käyttökelvottomaksi. Dark Avengerin katala tapa kirjoittaa satunnaisiin kohtiin levyä tekee niin ikään kohdalle sattuvat ohjelma- ja työtiedostot käyttökelvottomiksi. Disk killer kopioi alkuperäisen boot-lohkon ja osan itsestään levylle määrättyyn kohtaan välittämättä siitä, onko kohdalla ennestään jo tiedostoja. Alle jäävät ohjelmat ja työtiedostot lakkaavat toimimasta.

Jos ennen hyvin toiminut ohjelma tekee jonain päivänä lakon ja jää käynnistyksen jälkeen täysin jumiin, on virus yksi mahdollisuus monien muiden joukossa. Asialle voi olla luonnollinenkin selitys. Esimerkiksi kirjanpitotietojen (FAT) sekoaminen koko levyn tai vain kyseisen ohjelman kohdalta riittää tuottamaan saman ilmiön. Näyttöön tai sen ohjainkorttiin tullut vika riittää pimentämään näytön, vaikka ohjelma toimisikin. Ja niin edelleen, syitä on monia. Joka tapauksessa asia pitää tutkia.

Erityisen herkkiä viruksille ovat virusten tapaan toimivat muistinvaraiset (TSR) apuohjelmat. Niiden muistiin jääminen tai toiminta voi estyä, jos muistissa on jo virus.

Mikron toiminta hidastuu

Virus hidastaa koneen toimintaa, koska osa prosessorin ajasta kuluu viruksen ohjelmakoodin suorittamiseen. Normaalisti kuluva aika on niin vähäinen, ettei sitä havaitse ilman mittauksia. Hidastuminen voi kuitenkin muuttua näkyväksi silloin, kun virus tekee itsestään kopioita tai tutkii, onko asemaan laitettu levy jo saanut tartunnan vai pitäisikö se tartuttaa nyt. Jos levyke on kirjoitussuojattu, kuluu virukselta pitkä aika ennen kuin se huomaa yrityksensä turhiksi ja luopuu. Virus saattaa jopa "sahata" levykettä minuuttikaupalla ennen kuin se luopuu tartutta-

misesta ja käynnistää pyydetyn ohjelman. Levykkeiden toiminnan selvä hidastuminen onkin lähes varma merkki viruksesta.

Jerusalem-virukseen on tarkoituksella lisätty silmukka, jossa se alkaa kiertää oltuaan muistissa hieman vajaat 30 minuuttia. Silmukka kuormittaa perus-PC:tä niin paljon, että se lähes pysähtyy. Se lienee ollut alkuperäisen ohjelmoijan tarkoituskin. Nykyiset tehokkaat 286/386-koneet suorittavat silmukankin niin nopeasti, ettei käyttäjä yleensä huomaa hidastumista lainkaan.

Ohjelma ei enää mahdu muistiin

Jos aiemmin hyvin toiminut ohjelma antaa äkkiä ilmoituksen "Insufficient memory" eikä enää suostu käynnistymään, voi syynä olla virus, joka on kasvattanut ohjelmatiedoston koon niin isoksi, ettei se enää mahdu muistiin. Normaalisti virukset tarttuvat kuhunkin ohjelmatiedostoon vain kerran, mutta joistain viruksista tämä tarkistus puuttuu. Esimerkiksi Jerusalem-viruksen B-versiossa on ohjelmointivirhe, jonka vuoksi se kasvattaa ajettavan EXE-ohjelman kokoa jokaisella ajokerralla 1813 tavulla. Kun ohjelmaa on ajettu riittävän monta kertaa, on tiedoston koko kasvanut niin isoksi, ettei ohjelma mahdu muistiin. Viruksesta on liikkeellä myös versio, jossa tämä virhe on korjattu, mutta se on selvästi alkuperäistä virusta harvinaisempi.

Ellei ohjelman koko ole muuttunut, voi virheilmoitus aiheutua myös siitä, että vapaana oleva muisti on vähentynyt. Näin saattaa käydä, jos koneeseen asennetaan uusia muistinvaraisia apuohjelmia, lähiverkko tai laitteistokokoonpanoa muutetaan. Virheilmoitus voi siis johtua aivan luonnollisistakin syistä.

Alkulataus tapahtuu itsestään tai sen toiminta muuttuu

Muutamat virukset tuottavat joko tarkoituksella tai vahingossa kutsun, joka johtaa käyttöjärjestelmän uuteen lataamiseen, "buuttaukseen". Käytössä oleva ohjelma katkeaa, auki ollut työtiedosto menetetään ja mikro käynnistyy uudelleen alusta, aivan kuin näkymätön käsi olisi painanut CTRL-ALT-DELiä.

Joskus virus saattaa soittaa musiikkia tai tulostaa ruudulle viestejä kun käyttäjä itse painaa CTRL-ALT-DELiä. Kaikki tavallisuudesta poikkeavat ilmiöt alkulatauksen aikana onkin syytä tutkia.

Mikä ei (yleensä) ole virus?

Edellä kuvailtiin oireita, joita virukset aiheuttavat. Jos oireita alkaa tarkkailla liian kirjaimellisesti, on vaarana nähdä viruksia sielläkin missä niitä ei ole. Ilmiö on sama kuin lääkärikirjaa lukiessa: ennen pitkää lukija on varma, että hänellä on kaikki kirjassa kuvaillut taudit, siksi epämääräisiä ja yleisiä niiden kuvaukset ovat.

Viruksille on tyypillistä, että ne aiheuttavat selkeitä ja yksikäsitteisiä oireita. Bad sectorien määrän kasvaminen tai ohjelmatiedoston pituuden muuttuminen on lähes varma merkki viruksesta. Sen sijaan epämääräiset ongelmat, kuten levykkeiden sekoaminen tai mikron jääminen jumiin silloin tällöin johtuvat yleensä tavallisista laite- tai ohjelmavioista.

Valitettavasti tähänkään sääntöön ei voi aina luottaa. Koska viruksista pitää tehdä mahdollisimman pieniä, jää niihin helposti ohjelmointivirheitä ja yhteensopivuusongelmia. Hyvänä esimerkkinä tästä on alkuperäinen Ping-Pong-virus, joka toimii vain 8088-mikroissa viruksessa käytetyn harvinaisen konekielikäskyn vuoksi. Virukset ovat muutenkin hyvin laitesidonnaisia ja jos laitteistoa muutetaan, voivat virukset lakata toimimasta. Näin kävi mm. 3,5" korppuasemien yleistyessä. Virukset, jotka oli suunniteltu 5,25" levykkeitä varten, eivät toimineetkaan enää korpuilla, koska niiden sisäinen rakenne oli erilainen.

Virukset saattavat siten aiheuttaa epämääräisiä ongelmia, vaikkei se olekaan ollut ohjelmoijan alkuperäinen tarkoitus. Tämä tekee vaikeaksi erottaa milloin on kyseessä virus ja milloin jokin muu ongelma. Lisäksi on olemassa muutamia viruksia, jotka ovat suorastaan erikoistuneet epämääräisten vikojen aiheuttamiseen. Ne tuottavat tarkoituksella luku- ja kirjoitusvirheitä, sotkevat kirjoittimelle menevän tulostuksen, estävät ohjelmien toiminnan ja muuta ikävää.

Seuraavassa on esitelty ohjelmia ja tilanteita, joita usein virheellisesti luullaan virusten aiheuttamiksi.

Lost cluster

Yleisin DOSin CHKDSK-apuohjelman antamista ilmoituksista kuuluu seuraavaan tapaan:

```
10 lost clusters found in 2 chains
Convert lost chains to files (Y/N)?
```

Ilmoitus kertoo, että levyn kirjanpidosta on löytynyt varatuiksi merkittyjä alueita (chains, "ketjuja"), jotka eivät kuitenkaan näytä kuuluvan mihinkään olemassa olevaan tiedostoon. Alueet eivät ole varsinainen virhe, mutta ne varaavat turhaan tilaa joka voitaisiin käyttää hyödyllisemminkin. Tällaisia alueita syntyy helposti, mikäli koneesta katkaistaan sähköt kesken sovellusohjelman käytön. Ohjelma on ehtinyt varata itselleen tilaa levyltä, mutta ei ole vielä ehtinyt kertoa siitä levyn kirjanpidolle. Kun sähkö katkeaa, on levyn vapaasta tilasta pidettävä kirjanpito vain puolittain ajan tasalla.

Kun tällainen ilmoitus saadaan, pitää CHKDSK käynnistää uudelleen ja nyt /F-valitsinta käyttäen. Kysymykseen siitä, muutetaanko varatut alueet tiedostoiksi, voi yleensä vastata kielteisesti. Jos tiedostot halutaan luoda, syntyy jokaisesta ketjusta oma tiedosto päähakemistoon nimellä FILE000n.CHK, missä n on ketjun numero. Tiedostot voi poistaa sen jälkeen kun on tarkistanut, ettei niissä ole mitään hyödyllistä tietoa.

Oudot tiedostonimet

Levylle ilmestyvät oudot tiedostonimet saavat käyttäjän helposti epäilemään virusta. Tällaisten tiedostojen nimissä on satunnaisia numeroita ja kirjaimia, mutta tunnisteosaa niillä ei ole lainkaan. Tiedoston pituus saattaa olla nolla tai ainakaan TYPE-komento ei tulosta sen sisältöä ruudulle.

Tällaisia tiedostoja syntyy silloin, kun mikrossa ajettavat sovellusohjelmat luovat levylle tilapäisiä aputiedostoja. Antamalla tilapäisen tiedoston nimeksi satunnaisia kirjaimia ja numeroita varmistutaan siitä, ettei nimi mene päällekkäin levyllä jo olevien tiedostonimien kanssa. Kun tiedostoa ei enää tarvita, sovellus poistaa sen. Tiedostonimet saattavat kuitenkin jäädä näkyviin jos koneesta katkaistaan sähkö kesken ohjelman tai jos ohjelma jää jumiin. Tiedostojen pituuden kohdalla näkyvä nolla kertoo, ettei tiedostoa ole suljettu kunnolla.

Muita tilapäisen työtiedoston merkkejä ovat tunnisteosat TMP, $$$ sekä tiedostonimessä esiintyvät aaltoviivamerkit. Jos tällaisia tiedostoja ilmestyy levylle, kannattaa tarkkailla omia mikron käyttötottumuksiaan ja miettiä olisiko niissä korjaamisen varaa. Esimerkiksi sähköä ei saa katkaista ennen kuin kaikki ohjelmat on kunnolla lopetettu.

Käyttöjärjestelmä tarvitsee joskus itsekin tilapäistiedostoja. Kun käyttäjä antaa putkikomennon

```
C:\>DIR | SORT
```

tapahtuu seuraavaa: DIR tulostaa ensiksi hakemistoluettelon tilapäiseen tiedostoon, jonka käyttöjärjestelmä luo. Vanhoissa DOS-versioissa tiedostolle annetaan PIPE-alkuinen nimi; uudemmissa nimet ovat satunnaisia aakkos- ja numeromerkkejä. Tämän jälkeen SORT-ohjelma lukee aputiedoston, lajittelee sen, tulostaa luettelon ruudulle ja poistaa tarpeettomaksi käyneen aputiedoston. Sen nimi näkyy tulostuvassa listassa, koska tiedosto on ollut olemassa työn aikana, mutta kun työ on tehty, DOS poistaa sen.

Jos putkitoiminto jostain syystä keskeytetään, jää aputiedosto levylle.

Piilotetut tiedostot

Piilotettu tiedostonimi ei näy DIR-listauksessa. Tällaisten tiedostojen syntymistä levylle pidetään usein syyttä suotta viruksen merkkinä. Virus voi kyllä luoda levylle piilotettuja tiedostoja, mutta useimmiten asialla on ollut jokin sovellusohjelma tai itse käyttöjärjestelmä.

Piilotettujen tiedostojen lukumäärä on helppo selvittää CHKDSK-ohjelman avulla. CHKDSK laskee piilotettujen tiedostojen määrän kaikista hakemistoista. Jos levyllä on käyttöjärjestelmä, on piilotettuja tiedostoja vähintään kaksi. Levylle annettu nimi lasketaan myös yhdeksi piilotetuksi tiedostoksi. Esimerkiksi ilmoitus

```
45056 bytes in 3 hidden files
```

kertoo, että levyllä on kaksi piilotettua käyttöjärjestelmätiedostoa ja levylle on annettu nimi.

Kun CHKDSK-ohjelmalla katsotaan levykettä, jolla ei ole käyttöjärjestelmää, saattaa tuloslistassa näkyä arvoituksellinen rivi

```
0 bytes in 1 hidden files
```

Yksi piilotettu tiedosto, jonka pituus on nolla, tarkoittaa levyn nimeä (volum label). DOS 4.0:sta lähtien CHKDSK laskee levyn nimen piilotetuksi tiedostoksi vain, mikäli levyllä on myös käyttöjärjestelmä eikä tällaista hämäävää ilmoitusta tulostu.

Jos piilotettujen tiedostojen lukumäärä on suurempi kuin kolme, on levyllä ylimääräisiä piilotettuja tiedostoja. Monet apuohjelmat (kuten Nortonin FR) käyttävät niitä, samoin eräät sovellukset ja kopiosuojauksiin käytetyt menetelmät. Viruksista piilotettuja tiedostoja käyttävät vain harvat, vaikkei tätäkään mahdollisuutta voi kokonaan sulkea pois.

Yksi paljon piilotettuja tiedostoja luova ohjelma on 4DOSin mukana tuleva vaihtoehtoinen komentotulkki. Se kirjoittaa jokaiseen hakemistoon piilotetun DESCRIPT.ION-tiedoston, joka sisältää tiedostonimiin lisättyjä kommentteja.

EA DATA. SF

OS/2 käyttää 1.2-versiosta lähtien ns. laajennettuja tiedostomääreitä (extended attributes). Jokaiseen tiedostoon voidaan lisätä mm. kuvake, lyhyt kuvaus tiedoston sisällöstä, tiedoston tyyppi tai vaikka tekijän nimi. Koska näille tiedoille ei ole tilaa hakemistossa, on ne tallennetta-

va erikseen. OS/2 käyttää tallentamiseen levyn päähakemistoon luomaansa piilotettua tiedostoa, jonka nimi on EA DATA. SF (nimessä on todella välilyöntejä). Kun laajennettuja määreitä sisältäviä tiedostoja kopioidaan tai siirretään levyllä paikasta toiseen, päivitetään aina myös EA DATA. SF-tiedoston sisältöä. Tiedoston koko vaihtelee kiintolevyn koosta ja tiedostojen määrästä riippuen useista kymmenistä muutamaan sataan kilotavuun ja saattaa aiheuttaa ihmetystä, ellei käyttäjä tiedä tiedoston merkitystä.

Jos tiedostolle on annettu laajennettuja määreitä ja se kopioidaan levykkeelle, syntyy myös levykkeen päähakemistoon piilotettu EA DATA. SF-tiedosto, johon laajennetut määreet sijoitetaan. Jos tiedosto on jo olemassa, sen koko kasvaa. Levykkeellä tiedoston koko ei kuitenkaan koskaan pääse kasvamaan yhtä isoksi kuin kiintolevyllä.

DOS ja vanhemmat OS/2-versiot eivät ymmärrä laajennettuja määreitä. Ne eivät osaa päivittää EA DATA. SF-tiedoston sisältöä eivätkä siirtää määreitä tiedostojen mukana. Tämä ei kuitenkaan aiheuta OS/2:n kannalta mitään virhettä, vaan määreet yksinkertaisesti nollautuvat.

Windows 3:ssa on 386-koneissa mahdollista käyttää virtuaalimuistia, joka luo levylle ison piilotetun 386SPART.PAR-nimisen aputiedoston.

Out of file handles

Ohjelma, joka yhdessä koneessa toimii mainiosti, saattaa toisessa antaa virheilmoituksen "Out of file handles" tai toimia muutoin virheellisesti. Virheet liittyvät aina tiedostojen käsittelyyn, mutta saattavat ilmetä monin eri tavoin.

Virheilmoituksen syynä on liian pieni FILES-asetus. Asetus tehdään CONFIG.SYS-tiedostoon ja jotta ohjelmat toimisivat ongelmitta, kannattaa asetus tehdä kerralla riittävän isoksi kirjoittamalla

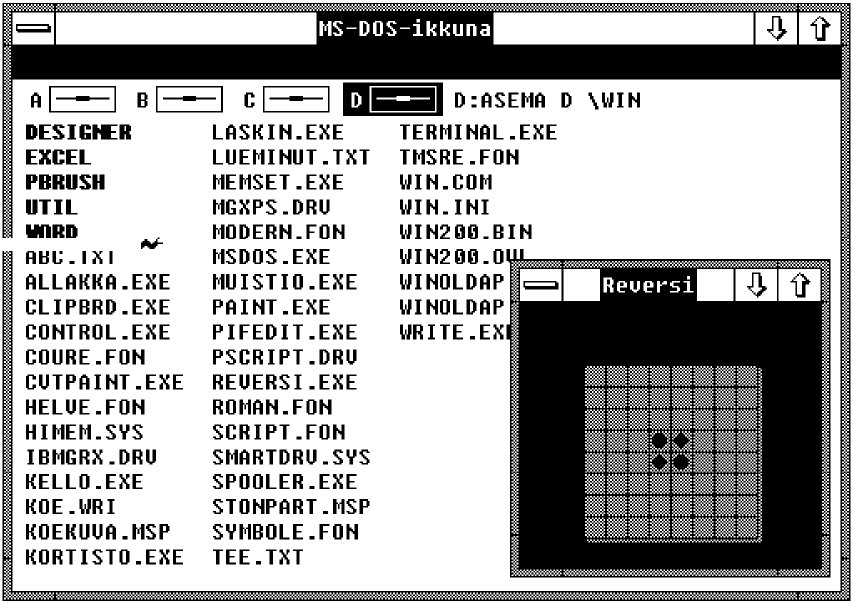
```
FILES=20
```

Suurempien lukuarvojen käytöstä ei perus-DOSissa ole mitään hyötyä, koska DOSissa oleva sisäinen rajoitus estää yhtä ohjelmaa avaamasta tätä useampia tiedostoja yhtä aikaa. Käytettäessä Windowsin kaltaisia moniajolaajennuksia on tiedostojen määrää syytä kasvattaa 30..50:een.

FILES-asetus voi jäädä liian pieneksi, mikäli käytetään esimerkiksi DOS 4.0:n omaa SELECT-asennusohjelmaa. Jostain käsittämättömästä syystä se varaa käyttöön vain 8 tiedostokahvaa, joka on aivan liian pieni määrä sovelluksia ajatellen.

Pilaohjelmat

Julkisessa levityksessä kiertää eräitä pilaohjelmia, jotka helposti sekoitetaan viruksiin. Ohjelmista näyttävin on Windowissa toimiva SLUG. Kun se käynnistetään, ei aluksi näytä tapahtuvan mitään. Jonkin ajan kuluttua ruudulle ilmestyy pieni mato, joka kiemurtelee ruudun poikki



Kuvaruudulla kulkeva mato näyttää todelliselta virukselta. Kyseessä on kuitenkin täysin harmiton pilaohjelma nimeltä SLUG.

ja vetää valkoista vanaa perässään. Hetken kuluttua mato ilmestyy esille uudesta kohtaa ja kulkee jälleen ruudun poikki. Kun ohjelma on kerran käynnistynyt, sitä ei saa mitenkään pysäytettyä. Ainoa tapa päästä eroon madosta on sammuttaa Windows ja käynnistää se uudelleen. Jos SLUGin käynnistyskomento on lisätty Windowsin omaan aloitustiedostoon WIN.INIin, ei tämäkään auta. Mato ilmestyy ruudulle heti kun Windows käynnistetään.

Toinen yleinen pilaohjelma on DRAIN.COM. Kun se käynnistetään, tulee ruudulle ilmoitus levyasemaan päässeestä vedestä, jonka ohjelma ilmoittaa kuivaavansa. Tämä tapahtuu linkousta muistuttavan ääniefektin kera.

```
A>  *** SYSTEM ERROR ***  # -031B

  Water detected in Drive A:

  Standby while water is drained

  Spin dry cycle starting  .....

  System OK now.... you may proceed.
```

CMOS-RAM

PC-koneissa on pieni muistialue, joka säilyttää tietonsa pariston tai akun varassa vielä virran katkaisun jälkeenkin. CMOS-muistissa pidetään mm. tietoa keskusmuistin koosta, levyasemien, näyttölaitteen ja kiintolevyn tyypeistä sekä kellonajasta ja päiväyksestä. Akun heikkeneminen tai 230-voltin linjalta tulleet jännitepiikit saattavat tyhjentää muistin, jolloin kone tuntuu menneen pahasti sekaisin. Se ei esimerkiksi tiedä päiväystä, ei löydä kiintolevyään eikä suostu siirtymään C: levyasemalle.

Onneksi tilanteesta on helppo toipua - ainakin, jos on osannut varautua asiaan. Esille kaivetaan DOSin sisältävä levyke ja kone käynnistetään sillä. Tämän jälkeen ajetaan koneen SETUP-ohjelma, joka löytyy joko diagnostiikkalevyltä tai koneen ROM-muistista. SETUP-

```
1. DATE:   24/06/1990
2. TIME:   08:46:15
3. FLOPPY  DRIVE A:  1.2M FLOPPY DRIVE
4. FLOPPY  DRIVE B:  1.44M FLOPPY DRIVE
5. FIXED   DISK  1:  TYPE 076
6. FIXED   DISK  2:  TYPE 021
7. PRIMARY DISPLAY:  SPECIAL ADAPTER
8. MEMORY BELOW 1 MEG. :   00640K
9. MEMORY ABOVE 1 MEG. :   03328K
A. COPROCESSOR.    : NOT PRESENT
B. UPDATE ALL ITEM
E. END AND REBOOT

SELECT WHICH ITEM ? _
```

Koneen SETUP kertoo mm. muistin, näyttölaitteen ja levyasemien tyypit. Kohdat 5 ja 6 kertovat koneessa olevien kiintolevyjen tyypit. Ne kannattaa kirjoittaa muistiin, koska lukujen selvittäminen jälkikäteen voi olla vaikeata.

ohjelmalla muistiin kirjoitetaan oikeat tiedot jonka jälkeen koneen käyttö voi taas jatkua normaalisti.

Ongelmia voi syntyä siitä, ettei monikaan käyttäjä tiedä, mikä numero kiintolevyn tyypin kohdalle pitäisi kirjoittaa. Asiaa on vaikeata selvittää jälkikäteen, sillä numerokoodi riippuu koneessa olevan kiintolevyn teknisistä parametreista ja vaihtelee vieläpä eri konemerkkien välillä. Jos tietää, montako levyä, uraa ja sektoria omalla kiintolevyllä on, voi oikeata koodia yrittää etsiä näiden tietojen perusteella. Usein ainoaksi mahdollisuudeksi jää soittaa maahantuojan huoltoon ja kysyä asiaa.

CMOS RAMin tyhjenemiseen voi varautua ennakolta kirjoittamalla muistiin SETUP-ohjelmassa näkyvät tiedot. Ne voi myös tulostaa hardcopynä paperille.

Levyaseman merkkivalon palaminen

Normaalisti kiintolevyn tai levykeaseman merkkivalon ei pitäisi palaa, ellei koneessa parhaillaan ajeta jotakin ohjelmaa. Tästäkin säännöstä on nykyisin niin monta poikkeusta, ettei valon vilkkumista voi pitää varmana merkkinä viruksesta.

Eräs luonnollinen syy valon vilkkumiseen voi olla lukupäiden suojaukseen käytetty muistinvarainen apuohjelma. Se siirtää lukupäät suojauralle heti kun mikro on ollut esimerkiksi 15 sekuntia käyttämättä. Kiintolevyn valo palaa siirron ajan ja sammuu sitten.

Lähiverkot, DOSin moniajolaajennukset ja PRINTin kaltaiset taustaohjelmat ovat tehneet yhä vaikeammaksi erottaa, milloin mikro tekee jotain ja milloin se on jouten. Merkkivalon vilkahtamista ei siis ainakaan kiintolevyllä voi automaattisesti pitää merkkinä lisääntyvästä viruksesta.

Selustan turvaaminen

Virusten torjuntastrategian viimeisen lenkin muodostaa selustan turvaaminen. Hoitamalla varmuuskopiointi tunnollisesti voidaan vahingon sattuessa minimoida menetykset - olipa syynä sitten tulipalo, varkaus, laitevika tai virus. Varmuuskopiointia on harrastettu niin kauan kuin tietokoneita on ollut olemassa, eikä siinä ole mitään uutta. Virusten uhka on vain hyvä syy tehdä varmistus entistäkin huolellisemmin.

Jokaiselle mikron käyttäjälle teroitetaan koulutuksen aikana mieleen varmuuskopioinnin merkitystä. Hyviä menetelmiä, ohjelmia ja periaatteita on olemassa lukuisia, eikä niihin puututa tässä kirjassa sen enempää. Seuraavassa kuitenkin eräitä näkökohtia, jotka liittyvät erityisesti viruksiin.

Pidä useita kopiosarjoja

Eräiden virusten kyky tuhota tiedostoja salakavalasti niin, ettei vahinko välttämättä näy ulospäin, pakottaa käyttämään useita kopiosarjoja. Varmistuksista pitäisi olla aina saatavilla myös yksi tai kaksi vanhempaa sukupolvea. Jos havaitaan, etteivät kaikki tiedostot ole kunnossa tuoreimmilla varmistuksilla, voidaan niitä palauttaa vanhemmilta sarjoilta.

Älä tee varmistuksesta liian perusteellista

Aina joskus näkee tapauksia, joissa varmistuksesta on tehty liiankin perusteellinen ja siten myös työläs. Käyttäjää on esimerkiksi neuvottu varmistamaan BACKUPilla koko kiintolevy aina perjantai-iltapäivisin. Tällainen varmistusrutiini alkaa helposti maistua puulta ja houkutus lintsaamiseen kasvaa. On parempi varmistaa tiedostoja usein ja pienissä erissä kuin harvoin ja silloin koko kiintolevy kerralla. Varmistus ei välttämättä tarkoita sitä, että tiedostot kopioidaan levykkeille. Pikavarmistuksia voi tehdä lähiverkon läpi toisille koneille tai omankin kiintolevyn sisällä hakemistosta toiseen. Kun tällainen varmistus liitetään komentojonon avulla jonkin sovelluksen käynnistämiseen, hoituu varmistus käyttäjän sitä edes huomaamatta.

Varmista, että myös palautus onnistuu

Varmistusten tekeminen ei vielä yksin riitä. Pitää myös tarkistaa, että tiedostojen palauttaminen onnistuu. Erityisen tärkeätä tämä on silloin, kun käytetään tallennusvälineitä, joissa tiedostojen kuntoa ei voi suoraan nähdä. Tällainen laite on esimerkiksi nauhavarmistusasema (streamer). Nauhan todellinen kunto selviää vasta kun tiedostoja yritetään palauttaa.

Jaa levy loogisiin asematunnuksiin

DOS 4.0:sta lähtien voidaan isokin levy ottaa käyttöön yhtenä C: tunnuksena. Tämä on harvoin järkevää. On paljon turvallisempaa jakaa asema 20-40 megatavun kokoisiin loogisiin levyasemiin (C:, D:, E: jne), jolloin ne saavat kukin oman kirjanpitonsa. Jos kirjanpitoon tulee jotain vikaa, rajoittuu vahinko vain kyseisen asematunnuksen kohdalle. Myös vahingossa poistetun tiedoston palauttaminen tai viruksen tekemien vahinkojen korjaaminen on sitä helpompaa, mitä pienempi asematunnuksen koko on.

Käytä oikeita apuohjelmia

Viruksia vastaan suunnattu varmuuskopiointi poikkeaa hieman perinteisistä varmistuksista. Tavallisestihan pyritään varmistamaan työtiedostot, jotta ne voitaisiin palauttaa mahdollisen levyvian tai muun onnettomuuden sattuessa. Koska monet virukset tuhoavat levyn sotkemalla sen kirjanpitoalueet tai kaikki uloimmat urat, pitäisi nämä alueet varmistaa tiedostojen lisäksi. Näin tehty varmistus täydentää mukavasti normaalia varmuuskopiointia ja sen voi lisätä jo olemassa olevan varmistusrutiinin jatkoksi. Nortonin FR, PC-Toolsin MIRROR ja Macen RXBAK ovat kaikki ohjelmia, jotka tekevät varmuuskopion FATeista ja päähakemistosta johonkin toiseen kohtaan levyä. Jos kirjanpito tuhoutuu, voidaan sen kopio ottaa käyttöön.

Apuohjelmia löytyy myös kokonaisten urien varmistamiseen. Osa niistä on PD-ohjelmia (kuten ST0 ja RT0), osa kaupallisia. Kaupallisista ohjelmista monipuolisin on HPERFin mukana tuleva pari GETSEC/PUTSEC, joista GETSEC lukee halutut urat/sektorit kiintolevyltä ja kirjoittaa ne levylle tiedostoon. PUTSEC palauttaa tiedoston haluttuun kohtaan kiintolevyä. Samantapaisia hyödyllisiä ohjelmia löytyy myös julkisohjelmina.

Niksejä virusten torjumiseksi

Virusten torjunta ei suinkaan vaadi kalliiden apuohjelmien hankkimista ja totuttujen käyttötapojen muuttamista. Pienillä nikseillä ja DOSin omilla apuohjelmilla voi huomattavasti parantaa mikronsa virusturvaa.

CHKDSKin kertomaa

DOSin mukana tulee erinomainen apuohjelma virusten torjuntaan: CHKDSK. Ohjelmaa pitää vain osata käyttää ja sen antamia ilmoituksia tulkita oikein. Se ei ole aivan helppoa, sillä CHKDSK-ohjelman tekijä oli tyypillinen atk-ammattilainen, joka ei viitsinyt tehdä ohjelmasta selkeätä tai yksinkertaista.

Ohjelman toimintaperiaatekin on monille PC-käyttäjille jäänyt hämäräksi. Se tiedetään, että ohjelma tutkii levyn kunnon, mutta miten tuo tutkiminen tapahtuu ja mitä se voi paljastaa - se onkin jo hämärän peitossa. DOSin käsikirjatkaan eivät ole kovin täsmällisiä CHKDSK:n toiminnasta kertoessaan.

Kun CHKDSK-ohjelman käyttöä aletaan tutkia huomataan, että nimi antaa aivan väärän kuvan sen toiminnasta. Parempi nimi tälle apuohjelmalle olisi CHKFAT. Kun CHKDSK-ohjelma ajetaan, se lukee FATit, katsoo ettei niissä ole loogisia virheitä ja vertaa niissä olevia tietoja hakemistoihin. CHKDSK tutkii siis kirjanpidon loogisen oikeellisuuden. Se ei huomaa, jos levylle on tullut uusia fyysisiä vikoja esimerkiksi levyn kulumisen tai äkillisen tärähdyksen vuoksi. CHKDSK kyllä kertoo vika-alueiden (bad sector) määrän, mutta tämä arvo lasketaan FATeihin tehdyistä merkinnöistä. Merkinnät on tehnyt levyn alustamiseen käytetty FORMAT-ohjelma. CHKDSK ei koskaan itse lisää bad sectorien määrää. Siihen pystyvät vain FORMAT ja RECOVER.

DOS 3.3-versioon asti tyypillinen CHKDSK-ajo näytti seuraavalta:

```
Volume CEE ASEMA   created 28 Mar 1990 8.29

 33400832 bytes total disk space
    53248 bytes in 3 hidden files
    65536 bytes in 23 directories
 21250048 bytes in 1089 user files
    20480 bytes in bad sectors
 12011520 bytes available on disk

   655360 bytes total memory
   586288 bytes free
```

DOS 4.0:sta lähtien CHKDSK ilmoittaa lisäksi levyllä käytetyn varausyksikön koon:

```
Taltio CEE ASEMA  , luotu 28.03.1990 8.29.

  33400832 tavua tilaa levyssä.
     53248 tavua 3 piilotiedostossa.
     65536 tavua 23 hakemistossa.
  21248000 tavua 1088 käyttäjätiedostossa.
     20480 tavua viallisissa sektoreissa.
  12013568 tavua käytettävänä levyssä.

Kussakin varausyksikössä on       2048 tavua.
Levyssä on      16309 varausyksikköä.
Levyssä on käytettävänä       5866 varausyksikköä.

Kokonaismuistitila     655360 tavua.
    571072 tavua vapaana.
```

Varausyksikön koko kertoo kirjanpidon käyttämän mittayksikön. Tällä levyllä se on 2048 tavua. Kiintolevyn koosta riippuen varausyksikön koko voi olla 2048, 4096 tai jopa 8192 tavua. Jos levy on alustettu OS/2:lla tai DOS 4:llä, tulostuu taltion nimen alle myös levylle alustuksen yhteydessä annettu sarjanumero.

Ylin numerorivi kertoo kiintolevyn tallennuskapasiteetin. Jos levy on jaettu useaan loogiseen levyasematunnukseen, luku kertoo tunnuksen koon. Kokonaiskapasiteetti saadaan laskemalla eri tunnusten luvut yhteen.

Piilotiedostojen määrä kiintolevyllä on yleensä vähintään kolme (kaksi käyttöjärjestelmätiedostoa + levyn nimi). Suurempi luku voi johtua kopiosuojatuista ohjelmista tai eräistä kiintolevyn käytön apuohjelmista, jotka näin piilottavat omaan käyttöönsä liittyvää tietoa.

Hakemistojen määrä ja niiden viemä tila selviää kolmannelta riviltä. Virustorjunnan kannalta tällä luvulla ei ole juurikaan merkitystä. Aina, kun levylle luodaan alihakemisto, varataan sille yhden varausyksikön verran tilaa. Jos tämä ei riitä, kasvattaa DOS automaattisesti hakemiston kokoa.

Seuraava rivi kertoo levyllä olevien tiedostojen kokonaismäärän sekä näiden viemän tilan. Viimeinen luku kertoo, paljonko levyn tilasta on vapaana. Väliin jäävä viallisten sektorien (oikeammin viallisten lohkojen) määrä on erittäin tärkeä. Sen ei pitäisi käytön aikana muuttua kumpaankaan suuntaan. Jos levyltä löytyy alustamisen yhteydessä vikaa, merkitsevät useimmat FORMAT-ohjelmat koko uran vialliseksi. Koska esimerkin levyasemalla on 17 sektoria, varataan jokaista vikaa kohti 8,5 kiloa - elleivät viat sitten satu samalle uralle. DOSin käyttämän kirjanpidon tarkkuus on esimerkissä 2 kiloa, joten pienin arvo, mihin vika-alueet kirjataan on 10 kilotavua. Vika-alueen koko onkin usein jokin 10 kilon kerrannainen. Esimerkin levyltä on löytynyt kaksi vikakohtaa, joten yhteensä vialliseksi on merkitty 20480 tavua.

Levykkeiden tarkistaminen CHKDSK:lla käy nopeasti. Pieni määrä vika-alueita saattaa johtua levykkeellä piileskelevästä viruksesta. Yhden kilotavun mittainen vika-alue johti tämän Ping-Pong viruksen paljastumiseen:

```
Taltio PC_UTILITY , luotu 28.07.1986 12.55.

    322560 tavua tilaa levyssä.
     40960 tavua 3 piilotiedostossa.
    266240 tavua 50 käyttäjätiedostossa.
      1024 tavua viallisissa sektoreissa.
     14336 tavua käytettävänä levyssä

Kussakin varausyksikössä on       1024 tavua.
Levyssä on        315 varausyksikköä.
Levyssä on käytettävänä         14 varausyksikköä.
```

```
Kokonaismuistitila     655360 tavua.
    573104 tavua vapaana.
```

Kaksi viimeistä CHKDSK:n kertomista luvuista liittyy keskusmuistiin ja ne ovat erittäin tärkeitä viruksia torjuttaessa. Ne kertovat, kuinka paljon perusmuistia koneessa on ja paljonko siitä on vapaana. Koska nykyisissä PC-koneissa on lähes poikkeuksetta 640 kilotavua perusmuistia, pitäisi ylemmän luvun olla 655360. Vapaan muistin koko saadaan vähentämällä tästä luvusta käyttöjärjestelmän viemä osuus, joka on yleensä 50-100 kiloa.

Eräissä koneissa pieni osa muistin yläpäästä on varattu koneelle itselleen tai siinä oleville lisäkorteille. Jos koneessa on ns. laajennettu BIOS, saattaa ylin kilo muistista puuttua. Tällöin muistia näyttää olevan vain 654256 tavua (639 kiloa). Eräissä HP:n koneissa varattua tilaa on neljän kilotavun verran, jolloin DOSille jää vain 651264 tavua. Muissa mikroissa saattaa esiintyä näistäkin poikkeavia lukemia.

Poikkeamista huolimatta molempia lukuja kannattaa seurata, sillä kun virus jää keskusmuistiin, vähenee muistin määrä viruksen itselleen varaaman tilan verran. Pudotus on helppo havaita, jos se liittyy ylempään lukuarvoon. Alempi, vapaana oleva muisti saattaa vaihdella käytetyistä DOS-apuohjelmista ja tehdyistä CONFIG.SYS-asetuksista riippuen joten sen seuraaminen on vaikeampaa.

Seuraavat arvot saatiin koneesta, jossa viruksia tutkittiin. Ensin vertailun vuoksi puhdas kone ilman viruksia:

```
Volume C ASEMA     created 30 Jan 1990 12.49

 33400832 bytes total disk space
    53248 bytes in 3 hidden files
    30720 bytes in 11 directories
  7278592 bytes in 340 user files
    30720 bytes in bad sectors
 26007552 bytes available on disk

   655360 bytes total memory
   586064 bytes free
```

Koska keskusmuistissa pesivät virukset vaikuttavat vain kahteen viimeiseen numeroon, on jatkossa listattu vain ne. Jos oman koneesi CHKDSK antaa samoja lukemia, on asia syytä tutkia.

Viruksista ensimmäisenä testattiin Yankee Doodlea. Se vähensi muistia seuraavasti:

```
652352 bytes total memory
583056 bytes free
```

Kooltaan hieman isompi ja vaikutuksiltaan paljon vaarallisempi Dark Avenger tuotti seuraavan ilmoituksen:

```
651664 bytes total memory
582368 bytes free
```

Stoned-virus vähentää muistia neljällä kilotavulla, jolloin ylempi muistilukema näyttää arvoa 651264. Määrä on sama kuin mitä eräissä HP:n mikroissa kuluu laajennetulle BIOSille mikä johtaa helposti vääriin hälyytyksiin.

Disk Killer piiloutuu levyn käynnistyslohkoon ja kiintolevyn nollauralle. Tutkituista viruksista se vei eniten keskusmuistia:

```
647168 bytes total memory
582944 bytes free
```

Riippuen siitä, miten virus on tehty, saattaa ylempi muistilukema säilyä ennallaan ja vain alempi vähentyä. Esimerkiksi yleinen Jerusalem B vaikuttaa ainoastaan vapaan muistin määrään:

```
655360 bytes total memory
584256 bytes free
```

Tämä tekee sen havaitsemisen pelkällä CHKDSKillä vaikeaksi.

CHKDSKin käyttö on helpompaa, mikäli muistin, piilotettujen tiedostojen ja bad sectorien normaaliarvot ovat muistissa joko paperille tulostettuna tai tiedostoon ohjattuna. Komento

```
C:\>CHKDSK C: >C:\DOS\CHKDSK-C.REF
```

luo \DOS-hakemistoon tiedoston CHKDSK-C.REF, josta näkyvät CHKDSK:n raportoimat normaaliarvot. Näitä on helppo verrata myöhempien CHKDSK-ajojen antamiin tuloksiin. Tällainen referenssitiedosto kannattaa luoda jokaiseen yrityksessä olevaan mikroon.

DEBUG

DEBUGilla voidaan tutkia keskusmuistin sisältöä tai ohjelmatiedostoja ennen niiden ajamista. Viruksen havaitseminen DEBUGin tuottamasta assembler-listauksesta edellyttää kuitenkin melkoista asiantuntemusta.

DEBUGista on silti hyötyä. Ellei mitään Nortonin tapaista apuohjelmaa satu olemaan ulottuvilla, voi sitä käyttää levyn käynnistyslohkon tutkimiseen. Lohkon sisältö saadaan näkyviin seuraavasti:

```
C:\DOS>DEBUG
- L DS:0a80 n 00 01
```

DEBUGin käynnistämisen jälkeen ruudulle tulostuu sen valmiusmerkkinä käyttämä miinus.L-komennon (Load) jälkeen annetaan esimerkissä näkyvät parametrit. N tarkoittaa levyaseman numeroa siten, että A-asema on nolla, B-asema yksi, C-asema kaksi jne.

L-komennolla DEBUG lukee lohkon keskusmuistiin. Se saadaan näkyviin D-komennolla:

```
-D DS:0A80
216B:0A80  EB 34 90 4D 53 44 4F 53-33 2E 33 00 02 01 01 00
.4.MSDOS3.3.....
216B:0A90  02 E0 00 60 09 F9 07 00-0F 00 02 00 00 00 00 00
...`............
216B:0AA0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 12
................
216B:0AB0  00 00 00 00 01 00 FA 33-C0 8E D0 BC 00 7C 16 07
.......3.....|..
216B:0AC0  BB 78 00 36 C5 37 1E 56-16 53 BF 2B 7C B9 0B 00
.x.6.7.V.S.+|...
216B:0AD0  FC AC 26 80 3D 00 74 03-26 8A 05 AA 8A C4 E2 F1
..&.=.t.&.......
```

```
216B:0AE0  06 1F 89 47 02 C7 07 2B-7C FB CD 13 72 67 A0 10
...G...+|...rg..
216B:0AF0  7C 98 F7 26 16 7C 03 06-1C 7C 03 06 0E 7C A3 3F
|..&.|...|...|.?
```

Sivun kapeuden vuoksi tulostus on jaettu kahdelle riville. Kuvaruudulla tekstit näkyvät heksakoodien perässä. Lohkon alussa lukee levyn alustamiseen käytetyn DOSin versiotunnus. Esimerkkilevyke on alustettu MS-DOS 3.3:lla. Jokainen D-komento tuo uudet 128 tavua näyttöön. Neljäs D-komento näyttää lohkon lopussa olevat tekstit:

```
-D
216B:0C00  74 65 6D 20 64 69 73 6B-20 6F 72 20 64 69 73 6B
tem disk or disk
216B:0C10  20 65 72 72 6F 72 0D 0A-52 65 70 6C 61 63 65 20
error..Replace
216B:0C20  61 6E 64 20 73 74 72 69-6B 65 20 61 6E 79 20 6B
and strike any k
216B:0C30  65 79 20 77 68 65 6E 20-72 65 61 64 79 0D 0A 00
ey when ready...
216B:0C40  0D 0A 44 69 73 6B 20 42-6F 6F 74 20 66 61 69 6C
..Disk Boot fail
216B:0C50  75 72 65 0D 0A 00 49 4F-20 20 20 20 20 20 53 59
ure...IO      SY
216B:0C60  53 4D 53 44 4F 53 20 20-20 53 59 53 00 00 00 00
SMSDOS   SYS....
216B:0C70  00 00 00 00 00 00 00 00-00 00 00 00 00 00 55 AA
..............U.
-Q
```

Kunnossa oleva käynnistyslohko on helppo tuntea siitä, että lohkon lopussa näkyvät käyttöjärjestelmän lataukseen liittyvät virheilmoitukset ("Non system disk or disk error"). Jos lohkon lopussakin on pelkkää ohjelmakoodia, on tämä usein merkki levyviruksesta.

Virustorjunta lähiverkossa

Lähiverkossa tulisi kaikki resurssit jakaa pelkin lukuoikeuksin. Näin voidaan varmistua siitä, ettei työasema vahingossakaan pysty kirjoittamaan verkon läpi palveluasemaan (serverille), josta saastunut tiedosto edelleen voi levitä kaikkiin muihin työasemiin.

Lähiverkon vastuuhenkilön (pääkäyttäjä) tulee tarkistaa jokainen ohjelma virusten varalta ennen sen kuin se asennetaan palveluasemaan.

Asemassa kannattaa myös ajaa silloin tällöin ohjelma, joka etsii levyltä mahdollisia viruksia. Ajon voi yhdistää palveluaseman normaalien ylläpitotoimien, kuten varmuuskopioinnin ja turhien tiedostojen poistamisen jatkoksi. Näin se tulee suoritettua automaattisesti ja huomaamatta.

Vastoin yleistä uskomusta virusten torjunta lähiverkossa on jopa helpompaa kuin yksittäisissä koneissa, sillä lähiverkon keskitetyt ylläpito- ja valvontamahdollisuudet auttavat suojaamaan järjestelmää. Toisaalta, ellei verkon ylläpitäjä hoida työtään kunnolla, on verkosta virusten leviämiselle vain pelkkää etua.

Omatekoiset komentojonot

Ohjelmatiedostojen pituuksia seuraamalla on helppo nähdä, milloin virus on tarttunut ohjelmaan. Seuraaminen on kuitenkin työlästä, joten se kannattaa automatisoida komentojonoja käyttämällä. Oheinen komentojono VIRTARK.BAT tarkistaa COMMAND.COMin pituuden ja antaa virheilmoituksen, mikäli sen pituus on muuttunut.

```
(1)    @ECHO OFF
(2)    DIR COMMAND.COM | FIND "25669" >TEMP1.TMP
(3)    COPY TEMP1.TMP TEMP2.TMP >NUL
(4)    IF EXIST TEMP2.TMP GOTO OK
(5)    ECHO Komentotulkin pituus on muuttunut!
(6)    ECHO Tarkista ettei asialla ole virus
(7)    :OK
(8)    IF EXIST TEMP2.TMP DEL TEMP2.TMP
(9)    DEL TEMP1.TMP
```

Komentojono toimii seuraavasti: Rivillä yksi estetään loppuja komentoja näkymästä antamalla asetus ECHO OFF. Rivillä kaksi pyydetään DIR-listaus komentotulkista ja etsitään listasta lukua 25669, joka on esimerkkikoneessa olevan komentotulkin oikea pituus. Jos luku löytyy, menee koko rivi TEMP1.TMP-nimiseen aputiedostoon. Ellei lukua löydy, komentotulkin pituus on muuttunut eikä TEMP1.TMP -tiedostoon mene mitään. Tiedosto syntyy levylle, mutta sen pituudeksi tulee nolla.

Kolmannella rivillä syntynyt tiedosto kopioidaan uudelle nimelle TEMP2.TMP. Vasta kopioimalla saadaan selville, onko tiedostossa jotain vai ei. Jos TEMP1.TMP-tiedoston pituus on nolla, ei kopiointi onnistu eikä TEMP2.TMP-tiedostoa synny lainkaan.

Neljännellä rivillä tutkitaan, onko tiedosto syntynyt ja jos on, on kaikki kunnossa. Komentotulkin pituus on täsmännyt rivillä kaksi annetun pituuden kanssa. Tällöin hypätään riville 7, jonka jälkeen poistetaan tarpeettomiksi käyneet aputiedostot TEMP1.TMP ja TEMP2.TMP. Virheilmoituksen välttämiseksi poistokäsky annetaan vain, jos tiedosto TEMP2.TMP on todella olemassa.

Jos TEMP1.TMP-tiedosto on jäänyt tyhjäksi, ei TEMP2.TMP -tiedostoa synny. Tällöin tulostetaan käyttäjälle varoitus, joka kertoo muuttuneesta pituudesta. Komentotulkin pituus ei normaalikäytössä muutu. Pituus voi muuttua vain, mikäli levykkeellä oleva tulkki kopioidaan vahingossa kiintolevyn päähakemistoon. Näin ei pitäisi koskaan tehdä, sillä väärää versiota oleva komentotulkki estää koneen toiminnan viimeistään seuraavan käynnistyksen yhteydessä. Varminta onkin suojata COMMAND.COM +R määreellä, jolloin sen päälle ei pysty vahingossakaan kopioimaan.

VIRTARK.BATin hyviä puolia ovat sen yksinkertaisuus ja nopeus. Tukihenkilö voi käydä lisäämässä sen jokaisen käyttäjän AUTOEXEC.BATiin, jolloin tarkistus tulee tehtyä automaattisesti aina kun mikro käynnistetään:

```
PATH C:\DOS;C:\DOS\KJONOT
KEYB SU,,C:\DOS\KEYBOARD.SYS
PROMPT $P$G
CALL VIRTARK
REM ... loput komennot tähän ...
```

CALL-käsky toimii vain DOS 3.3:sta alkaen. Tätä vanhemmissa versioissa pitää käyttää muotoa COMMAND/C VIRTARK.

VIRTARK-komentojonoa voi täydentää monin tavoin. COMMAND.COMin lisäksi voidaan tarkistaa yleisimpien sovellusohjelmien pituudet. Esimerkiksi WP:n pituuden tarkistamiseksi muutetaan riviä 2 seuraavasti:

PC-DOS	pituus	päiväys	kieli
3.2	23791	30.12.85	englanti
3.3	25307	17.03.87	englanti
4.0	37637	17.06.88	englanti
4.0	38457	29.08.88	suomi

Komentotulkin COMMAND.COM pituus ja päiväys eräissä PC-DOS-versioissa. MS- DOSin arvot saattavat poiketa näistä jonkin verran. Kahta muuta piilotettua DOS-tiedostoa (IBMDOS/IBMBIO tai MSDOS/IO) ei yleensä kannata seurata, koska vain harvat virukset tarttuvat niihin.

```
(2)    DIR C:\WP\WP.EXE | FIND "xxxxxx" >TEMP1.TMP
```

Lainausmerkkien sisään kirjoitetaan oman WP-version pituus.

Vielä käyttökelpoisempi tarkistuksesta saadaan, jos se suoritetaan aina ohjelman käynnistämisen yhteydessä. Esimerkiksi WP:n tapauksessa tehdään komentojono W.BAT, joka näyttää seuraavalta:

```
(1)    @ECHO OFF
(2)    DIR WP.EXE | FIND "261669" >TEMP1.TMP
(3)    COPY TEMP1.TMP TEMP2.TMP >NUL
(4)    IF EXIST TEMP2.TMP GOTO OK
(5)    ECHO WP:n pituus on muuttunut! Kutsu
(6)    ECHO mikrotukihenkilö paikalle
(7)    GOTO ULOS
(8)    :OK
(9)    IF EXIST TEMP2.TMP DEL TEMP2.TMP
(10)   DEL TEMP1.TMP
(11)   WP %1 %2 %3
(12)   :ULOS
```

Jos WP:n pituus ei täsmää, komentojono neuvoo kutsumaan mikrotukihenkilön paikalle eikä käynnistä ohjelmaa. Komentojono kannattaa kopioida tärkeimmille sovellusohjelmille ja muuttaa ohjelman pituus- ja nimitiedot niiden tietoja vastaaviksi. Loppuun voi vielä lisätä osuu-

den, joka kopioi kaikki muuttuneet työtiedostot automaattisesti toiseen hakemistoon kun sovellus päättyy.

Vapaan keskusmuistin koko ja kiintolevyllä olevien bad sectorien määrä saadaan tarkistettua samalla periaatteella, mutta nyt DIR-käskyn tilalla käytetään CHKDSK-ohjelmaa. Rivi

```
(2)   CHKDSK C:|FIND "10240 bytes in bad" >TEMP1.TMP
```

tarkistaa, että CHKDSK löytää levyltä 10240 tavua bad sectoreita.

Jos kirjanpidosta löytyy virheitä, CHKDSK antaa niistä ilmoituksen ja pysähtyy odottamaan käyttäjältä kuittausta. Virheen löytyminen pysäyttää siis myös komentojonon. Lisäksi kirjanpidon tarkistaminen voi kestää jonkin aikaa. Näistä syistä keskusmuistin koon tarkistamiseen kannattaa mieluummin käyttää MEM-ohjelmaa tai jotain sen julkisohjelmavastinetta, ellei koneessa ole DOS 4.0:aa.

Edellä kuvattuja komentojonoja ei kannata luoda, jos virus on jo päässyt koneeseen. COMMAND.COMia tai sovellusten pituuksia on turha verrata, jos alkuperäinenkin vertailuluku on viruksen saastuttama. Koneen puhtaus pitääkin varmistaa esimerkiksi virusten etsintäohjelmia käyttäen ennen kuin komentojonot asennetaan käyttäjille.

Pituuksia tarkistavista komentojonoista ei myöskään ole hyötyä uusia tehoviruksia vastaan, jotka osaavat peittää tiedostojen kasvamisen niin, ettei se näy edes käyttöjärjestelmälle. Näitä viruksia on tarkasteltu luvussa kahdeksan.

5

Virukset ja muut tietokoneet

Edellisissä luvuissa on kerrottu viruksen elämästä lähinnä PC-koneiden DOS-käyttöjärjestelmässä. Viruksia on kuitenkin löydetty lähes kaiken tyyppisistä mikroista, kotimikroista isoihin tietokoneisiin asti. Tässä luvussa tarkastellaan lyhyesti muita kuin DOS-viruksia.

Isojen tietokoneiden virukset

Mikään tietokone ei ole täysin turvassa viruksilta. Isoissa keskuskoneissa vaara viruksen saamiseen on kuitenkin merkittävästi pienempi kuin mikroissa. Tähän on monta syytä.

Tärkein syistä on se, että isoja tietokoneita pääsevät ohjelmoimaan vain alan koulutetut ammattilaiset. Nämä yleensä kypsässä iässä olevat henkilöt eivät ole kiinnostuneita viruskokeiluista, eikä heillä olisi siihen aikaakaan. Muutakin työtä tietokoneen parissa riittää ja siitä jopa maksetaan.

Viruksen tekeminen vaatii aina koneen perusteellista tuntemista. Isot koneet on tehty valmistajan omaa, suljettua tekniikkaa käyttäen, eivätkä ne ole yhteensopivia muiden valmistajien koneiden kanssa. Ohjelmointioppaita tai koneen rakenteesta kertovia kirjoja saa ainoastaan koneen valmistajalta. Niitä ei myydä mikrokirjojen tapaan jokaisessa kirjakaupassa.

Isoon tietokoneeseen tehdyn viruksen olisi vaikeata levitä koneesta toiseen. Operaattorit kun eivät kuljeta ohjelmien magneettinauhoja salkussaan eivätkä käy ajamassa niitä kollegojensa koneissa. Yhteen

koneeseen tehty virus todennäköisesti myös jäisi siihen, jolloin sen tekijää ei tarvitsisi etsiä kaukaa.

Viruksia ei kannata edes suunnitella, koska isojen tietokoneiden turvallisuusriskit on tiedostettu jo kauan sitten ja koneiden käyttöä valvotaan tarkasti. Käyttöjärjestelmään on lisätty omat toiminnot valvontaa ja käytön seurantaa varten. Vaikka viruksen voisikin ujuttaa järjestelmään, jäisi siitä aina jälkiä, joiden perusteella tekijä saataisiin selville.

Näillä näkymin ei ole suurtakaan pelkoa siitä, että virus tuhoaisi pankin tilitiedot tai poliisin rikosrekisterin. Moninkertaisten varmistusten ja useiden käyttöä valvovien henkilöiden vuoksi vaadittaisiin kokonainen salaliitto, ennen kuin järjestelmää voitaisin sabotoida tai siihen istuttaa tarkoituksella tehty virus.

Täysin varmoja eivät ole isotkaan tietokoneet. Sen osoitti konkreettisesti IBM:n joulukorttivirus.

Joulukorttivirus

Joulukorttivirus lähti leviämään joulun alla 1987 Länsi-Saksan Clausthalista. Virus oli koodattu VM-käyttöjärjestelmän REXX-kielellä (vastaa DOSin komentojonoja) ja se levisi EARN/Bitnet-verkossa koneesta toiseen elektronisen postin välityksellä.

Utelias käyttäjä, joka halusi tutkia postin tuoman REXX-ohjelman sisältöä, löysi sen alusta ohjeet, jotka neuvoivat vain käynnistämään ohjelman ja nauttimaan sen ajosta. Näin ei tietenkään pitäisi koskaan tehdä, mutta vuonna 1987 monet käyttäjät olivat vielä niin sinisilmäisiä, että noudattivat neuvoa.

Kun ohjelma oli käynnistetty komennolla CHRISTMAS, tulostui päätteelle yksinkertainen joulukortti:

```
              *
              *
             ***
            *****
           *******
          *********
         ***********
        *************              A
           *******
         ***********             VERY
      *****************
     *******************         HAPPY
         ***********
       ***************         CHRISTMAS
     *******************
   ***********************       AND MY
       ***************
     *******************      BEST WISHES
  ************************
****************************  FOR THE NEXT
            *****
            *****                 YEAR
            *****
```

Kun joulukuusi oli tulostettu ruudulle, virus tarkisti koneen päivämäärän. Jos se oli suurempi kuin tammikuu 1988, ohjelma loppui. Näin tekijä oli varmistanut ettei virus pääsisi leviämään holtittomasti. Jos elettiin joulukuuta 1987 tai tammikuuta 1988, virusohjelma kävi tutkimassa käyttäjän elektronisen postiluettelon ja lähetti kopion itsestään tässä listassa mainituille vastaanottajille. Virus levisi nopeasti moniin maihin aina Suomea ja Japania myöten. Ketjureaktion tapaan levinnyt virus johti monen koneen ylikuormittumiseen.

Vaikka isot tietokoneet ovatkin turvallisempia kuin henkilökohtaiset mikrot, ovat niidenkin valmistajat ottaneet virusuhkan vakavasti. Esimerkiksi IBM on kehitellyt isoille koneilleen ohjelmia, jotka tarkistussummien avulla havaitsevat ohjelmatiedostoissa mahdollisesti tapahtuvat muutokset.

Virukset ja OS/2

OS/2 on DOSia monin tavoin kehittyneempi käyttöjärjestelmä. Se pystyy ajamaan monta ohjelmaa yhtä aikaa ja osaa käyttää paljon isompaa muistia kuin DOSin tuntema 640 kilotavua. Graafinen käyttöliittymä täydentää kokonaisuuden ja eristää käyttäjän levyn tekniikasta.

OS/2:ssa oleva moniajo tekee virusten leviämisen helpoksi. Virus voi olla koko ajan käynnissä muiden prosessien tapaan eikä sen tarvitse varastaa itselleen keskeytyksiä kuten DOSissa. Itse asiassa OS/2:ssa ei edes ole keskeytyksiä. Viruksen on myös helpompaa tehdä itsestään kopioita. Tausta-ajossa ollessaan se voi milloin tahansa käydä lukemassa ja kirjoittamassa levykkeitä.

OS/2:een on kuitenkin rakennettu suojauksia, joiden tarkoituksena on eristää eri prosessit toisistaan, olivatpa ne sitten sovellusohjelmia tai viruksia. Suora kirjoittaminen levylle, jolla on avonaisia tiedostoja, on niin ikään estetty. Käytännössä tämä tarkoittaa sitä, ettei mikään ohjelma pysty suoraan kirjoittamaan C: aseman varatuille alueille eikä siten myöskään piilottamaan levylle mitään. Suojaus on niin tehokas, ettei edes OS/2:n oma CHKDSK pysty korjaamaan FATiin tulleita virheitä!

Suojaukset eivät ulotu laiteohjaimiin, jotka ladataan muistiin CONFIG.SYS-tiedostossa. Nämä ohjaimet pystyvät kirjoittamaan suoraan levylle ja muutenkin käsittelemään resursseja omavaltaisesti. Epämääräisistä lähteistä peräisin olevia ohjaimia ei kannata tästä syystä käyttää.

OS/2 ja DOS-tila

DOSia varten tehdyt ohjelmat, olivatpa ne sitten viruksia tai hyötysovelluksia, eivät sellaisenaan toimi OS/2:ssa. Ohjelmat pitää varta vasten kirjoittaa käyttämään moniajoa, virtuaalimuistia ja muita OS/2:n tarjoamia hienouksia. Yhteensopivuuden säilyttämiseksi OS/2:een on kuitenkin lisätty ns. DOS-tila, jossa vanhoja DOS-ohjelmia voidaan yhä ajaa. Tilassa toimivat lähes kaikki DOSille tehdyt ohjelmat - myös sellaiset perusvirukset kuten Jerusalem, Yankee Doodle, Vacsina.

Dark Avenger -virus yrittää käyttää levyn käynnistyslohkoa sisäiseen kirjanpitoonsa. Koska OS/2 estää suorat kirjoitukset levyn varatuille alueille, ei Dark Avenger pääse alkua pitemmälle. Samoin käy 1701-virukselle. OS/2 keskeyttää sen heti, kun virus yrittää muuttaa keskeytysosoitetta.

Ne virukset, jotka toimivat, pystyvät kyllä lisääntymään OS/2:n DOS-tilassa, mutta eivät juurikaan tuottamaan vahinkoa. Virus ei pysty alustamaan kiintolevyä eikä tuottamaan muutakaan merkittävää vahinkoa, koska käyttöjärjestelmä estää tällaiset yritykset.

Käynnistyslohkoon kiinnittyvistä viruksista ei tarvitse välittää, sillä OS/2 voidaan käynnistää vain kiintolevyltä, eikä sen käynnistyslohkoon tarttunut DOS-virus selviäisi latausvaiheesta.

OS/2:ssa voidaan tehdä ns. perheohjelmia. Nämä ohjelmat näyttävät ulospäin tavallisilta EXE-tiedostoilta, mutta niitä voidaan ajaa sekä OS/2:ssa että DOSissa. Varsinaisen koodin lisäksi perheohjelman sisältä löytyy pieni osa kumpaakin käyttöjärjestelmää varten. Perhe-nimi viittaa Microsoftin käyttöjärjestelmäperheeseen.

Lähes kaikki OS/2:n apuohjelmat (CHKDSK, ATTRIB, TREE jne) ovat perheohjelmia jolloin niitä voidaan ajaa sekä aidossa OS/2- tilassa että DOS-tilassa. Koska perheohjelmien EXE-tiedostorakenne poikkeaa DOSin käyttämästä, eivät DOS-virukset osaa tarttua niihin. Vaikka DOS-tilassa olisikin virus, voidaan apuohjelmia ajaa normaaliin tapaan.

Virukset ja Windows

Vaikka Windows käynnistetään sovellusohjelman tapaan, on se kuitenkin aivan oma käyttöjärjestelmänsä. DOSin palveluita Windows käyttää vain tiedostojen käsittelyyn. Moniajosta, muistinhallinnasta ja oheislaitteiden ohjauksesta Windows 3 huolehtii itse ja se tarjoaa nämä palvelut myös kaikille Windows-sovelluksille. Windowsin 3-versio pystyy rikkomaan DOSin 640 kilotavun rajoituksen, koska se käyttää OS/2:n tavoin prosessorin suojattua tilaa.

Microsoft aloitti Windowsin kehittelyn vuonna 1983. Ensimmäinen versio tuli myyntiin loppuvuodesta 1985. Kaupallista merkittävyyttä

Windows alkoi saada vasta 1980-luvun lopulla ja 22.5.1990 tapahtunut Windows 3.0-julkistus teki siitä houkuttelevan vaihtoehdon merkkipohjaisille DOS-sovelluksille. Ainakin lyhyellä tähtäyksellä katsottuna Windowsista oli tullut se, mitä OS/2:sta oli odotettu.

Windowsin käyttäminen on DOSin käyttöä turvallisempaa. Koska Windowsin EXE-tiedostojen rakenne muistuttaa enemmän OS/2:ta kuin tavallista DOSia, eivät useimmat DOS-virukset osaa tarttua niihin oikein. Erityisten Windows-virusten tekeminen on vaikeata, sillä Windows-ohjelmointi poikkeaa täysin DOS-ohjelmoinnista. Sen opiskeleminen vaatii asiaan paneutumista ja uusien työkalujen hankkimista. On silti hyvin todennäköistä, että Windowsin yleistymisen myötä tullaan jonain päivänä näkemään ensimmäiset Windows-virukset.

Virukset ja Amiga

Commodoren Amiga julkistettiin suurella kohulla kesällä 1986. Aikansa PC-koneisiin verrattuna Amigassa oli tehokkaampi prosessori ja DOSia selvästi kehittyneempi, yksinkertaiseen moniajoon pystyvä käyttöjärjestelmä. Ominaisuuksistaan huolimatta Amigasta ei ole tullut vakavasti otettavaa vaihtoehtoa Macintoshille tai PC:lle.

Amigan käyttöliittymä on Macin tapaan graafinen, mikä helpottaa virusten tekemistä. Suurin osa Amigoista on hankittu koti- ja pelikäyttöön, jolloin suurin osa ohjelmista saadaan kavereilta vaihtamalla. Laiton kopiointi levittää tehokkaasti viruksia. Suurin osa Amigan viruksista piiloutuu käynnistyslohkoon, jolloin ne pääsevät muistiin heti kun kone käynnistetään.

Tunnetuin Amigan viruksista on nimeltään SCA. Virus on saanut nimensä tekijästään (Swiss Cracking Association), joka loi viruksen käytännön pilaksi ja sai sen leviämään muutamassa kuukaudessa ympäri maailman. Harmiton SCA-virus tunnetaan parhaiten tekstistä, jonka se esittää silloin tällöin koneen käynnistämisen yhteydessä: "Something wonderful has happened - your Amiga is alive..." (Suomeksi: "Jotain ihmeellistä on tapahtunut - Amigasi on herännyt eloon..."). Muita harmittomia mutta helposti leviäviä viruksia ovat mm. Byte Warrior, North Star ja Pentagon Circle.

Byte Bandit kopioi itsensä kaikille levykkeille, joita asemaan laitetaan. Kun virus on tehnyt itsestään kopion, se kaataa koneen viiden minuutin välein.

IRQ-virus tarttuu ajettaviin ohjelmiin. Se ei tee vahinkoa, mutta tuottaa yhteensopivuusongelmia uusien käyttöjärjestelmäversioiden kanssa.

Lamer Exterminator on nimensä mukaisesti suunnattu sellaisia henkilöitä vastaan, jotka keräävät ja levittävät laittomasti kopioituja ohjelmia. Virus koodaa itsensä niin, että sitä on vaikeata havaita. Kun virus on tehnyt itsestään kolme kopiota, se täyttää yhden levykkeen sektoreista "LAMER!" -tekstillä ja tuhoaa näin alle jäävän tiedoston.

Virukset ja Macintosh

Vaikka Macintosh-viruksia tunnetaan kappalemääräisesti vähemmän kuin PC-viruksia, on saastuneiden mikrojen prosenttiosuus Mac-puolella selvästi PC:tä korkeampi. Tähän on monia syitä. Mac-ohjelmia kopioidaan enemmän kuin PC-ohjelmia, jolloin virusten leviäminen on helpompaa. Lisäksi Macejä käytetään paljon kouluissa ja oppilaitoksissa, joissa ohjelmat ja levykkeet kiertävät kädestä käteen.

Macin graafinen käyttöliittymä on näyttävä ja suorastaan houkuttelee pilavirusten tekemiseen. Grafiikka eristää käyttäjän laitetasosta niin hyvin, että useimmilla koneen käyttäjillä ei ole aavistustakaan ohjelmatiedostojen pituuksista tai muista teknisistä seikoista. Macin filosofiana on, ettei käyttäjää pidä rasittaa turhilla teknisillä yksityiskohdilla. Tärkeintä on, että kone ja sen ohjelmat auttavat käyttäjää hoitamaan työnsä entistä tehokkaammin.

Kaikesta tästä seuraa, että vaikka Mac-viruksia tunnetaankin kappalemääräisesti vähän, ne ovat levinneet hyvin laajalle. Myös Suomessa Mac-virukset aiheuttivat epidemioita paljon ennen PC-viruksia.

Jostain syystä lähes kaikki Mac-virukset ovat hyväntahtoisia, ts. ne eivät tarkoituksella tuota vahinkoa. Koska eri Mac-mallit poikkeavat melkoisesti toisistaan ja käyttöjärjestelmästäkin on liikkeellä monia eri versioita, ovat yhteensopivuusongelmat ja tahattomat häiriöt sitäkin yleisimpiä.

Seuraavassa on lueteltu yleisimmät Mac-virukset.

Scores. Scores-virus löydettiin keväällä 1988. Virus tarttuu järjestelmätiedostoihin, muistilehtiöön sekä leikekirjaan. Lisäksi se luo järjestelmäkansioon kaksi piilotettua tiedostoa nimillä "Scores" (josta virus on saanut nimensäkin) ja "Desktop " (nimessä on yksi välilyönti p:n jälkeen). Kaksi päivää sen jälkeen, kun virus on päässyt koneeseen, se alkaa levitä ja tarttuu useimpiin ajettaviin ohjelmiin. Tartunta tapahtuu 2-3 minuuttia ohjelman käynnistyksen jälkeen.

Scores-virus ei aiheuta tarkoituksellista vahinkoa. Se saattaa kuitenkin haitata tulostamista mm. Excelistä ja MacDraw-ohjelmasta sekä aiheuttaa muitakin epämääräisiä oireita. Virus on helppo havaita, sillä normaalisti pieniltä Maceiltä näyttävät leikeikirjan ja muistilehtiön ikonit muuttuvat viruksen jäljiltä tyhjän paperin ikoneiksi. Virus saattaa tarttua vain osittain, jolloin ikonit jäävät ennalleen.

Scores ja nVIR lienevät Macin yleisimpiä viruksia. Siksi useimmat torjuntaohjelmat havaitsevat ne ongelmitta.

nVIR. Ensimmäiset havainnot nVIR-viruksesta tehtiin 1987. Virus tarttuu järjestelmätiedostoon ja aloittaa leviämisensä välittömästi. Se tarttuu käynnistettäviin ohjelmiin, mutta Scores-viruksen tavoin eräät ohjelmatiedostot olla sille immuuneja, jolloin tartunta ei onnistu. Viruksesta on olemassa ainakin kaksi versiota, nVIR A ja nVIR B. Jälkimmäisestä B-versiosta tunnetaan lisäksi monta eri muunnelmaa. Viruksen nimi tulee sen perustamasta "nVIR" resurssityypistä.

Kun nVIR A-versio tarttuu järjestelmätiedostoon, se perustaa laskurin, jonka alkuarvo on 1000. Aina, kun kone käynnistetään, laskurin arvoa vähennetään yhdellä. Jokainen viruksen saastuttaman ohjelman ajokerta vähentää arvoa kahdella. Kun laskuri saavuttaa arvon nolla, koneen kaiuttimesta kuuluu ääni "Don't panic" jos MacinTalk on asennettu tai pelkkä äänimerkki, ellei sitä ole. Sama efekti tapahtuu 1/16 todennäköisyydellä koneen käynnistyksen yhteydessä ja todennäköisyydellä 15/128 aina kun tartunnan saanut sovellus käynnistetään.

B-versiossa toiminta on hieman erilaista. Kaiuttimesta kuullaan pelkkä äänimerkki ja todennäköisyydet ovat hieman toiset.

Erikoisinta nVIR-viruksissa on niiden kyky tuottaa jälkeläisiä. Jos koneessa on nVIR A-virus ja siinä ajetaan nVIR B:n saastuttamaa ohjelmaa, osa viruksen koodista korvautuu nVIR A:n koodilla. Näin syntynyt virus sisältää sekä A- että B-viruksen koodia, mutta käyttäytyy A-tyypin tavoin. Vastaavasti, jos koneessa on B-tyypin virus ja siinä ajetaan A-tyypin saastuttama ohjelma, korvautuu osa viruksesta B-tyypin koodilla ja lopputuloksena on B-tyypin tapaan käyttäytyvä virus. Näin syntyneet uudet virukset ovat sikäli uusia, että etsintäohjelmien on vaikeata tunnistaa niitä. Uusia viruksia voi myös "risteyttää" alkuperäisten vanhempiensa kanssa, jolloin tuloksena on jälleen uudenlaisia viruksia. Todellista mikrobiologiaa!

Äänimerkkejä ja satunnaisia yhteensopivuusongelmia lukuunottamatta nVIR ei aiheuta koneelle vahinkoa. NVIRin pohjalta on tehty ainakin seitsemän erilaista versiota, mm. HPAT-, MEV#- ja AIDS-virukset. Joidenkin näistä tiedetään tuhoavan levyn tiedostoja.

MacMag. Macintosh II:n julkistamispäivän "kunniaksi" tehty virus, joka tuli kuuluisaksi päästyään valmisohjelmalevykkeelle ja levittyään tästä syystä erittäin laajalle. Koska MacMag tuhosi itsensä 2.3.88, ei sitä pitäisi enää olla missään liikkeellä.

ANTI. Ranskasta vuoden 1989 alussa löydetty virus, joka muista poiketen ei tartu lainkaan järjestelmätiedostoon vaan ainoastaan sovelluksiin. Teknisistä syistä johtuen ANTI ei toimi Multifinderin kanssa. Virus on saanut nimensä merkkijonosta, joka löytyy viruksen ohjelmakoodin keskeltä. Virus ei aiheuta suoranaista vahinkoa.

INIT 29. Erittäin helposti tarttuva virus, joka löydettiin vuoden 1988 lopussa. Virus on saanut nimensä käyttämästään INIT-resurssityypistä ja ID-tunnuksesta 29. Virus tarttuu suoraan levyllä oleviin tiedostoihin, niin käyttöjärjestelmään, sovelluksiin kuin työtiedostoihinkin. Työtiedostoihin tarttuneet virukset eivät kuitenkaan pysty tartuttamaan uusia tiedostoja.

INIT 29-virus ei aiheuta suoranaista vahinkoa, mutta tuottaa usein epämääräisiä ongelmia Multifinderin ja tulostusohjelmien kanssa.

WDEF. Virus löydettiin joulukuussa 1989 Belgiassa ja se on sen jälkeen levinnyt hyvin laajalle. Viruksesta on liikkeellä sekä A- että B-versiota. Versiot ovat hyvin samanlaisia. Ainoa ero niiden välillä on, että B-versio tulostaa äänimerkin aina kun se tarttuu uuteen levyyn.

WDEF tarttuu vain piilotettuihin työpöytätiedostoihin, joita Finder käyttää. Virus ei tartu ohjelmiin vaan leviää ainoastaan levyjen välityksellä. Näin sen toiminta muistuttaa PC-koneiden levykeviruksia.

Virus ei aiheuta suoranaista vahinkoa, mutta se ei toimi kunnolla kaikissa Macintosh-malleissa. Esimerkiksi portable- ja Mac IIci-koneissa se jumiuttaa koneen lähes välittömästi saastuneen levykkeen käytön jälkeen. Muissakin malleissa se aiheuttaa epämääräisiä toimintahäiriöitä, jotka saattavat ilmetä mm. fonttien käsittelyssä. TOPS-verkossa virus voi levitä serveristä työasemaan.

MDEF. Tämä Cornellin yliopistolta toukokuussa 1990 löytynyt virus tunnetaan myös nimellä "Garfield". Virus tarttuu sekä käyttöjärjestelmätiedostoon että sovelluksiin. Viruksen ei tiedetä aiheuttaneen mitään vahinkoa eikä se aiheuta edes mitään pilaefektiä. Se vain leviää.

Teknisistä syistä johtuen MDEF ei toimi vanhoissa 128 ja 512 kilon Mac-malleissa. Nimestään huolimatta viruksella ei ole mitään yhteistä WDEFin kanssa.

ZUC. ZUC-virus havaittiin ensi kertaa Italiassa maaliskuussa 1990. Virus on saanut nimensä löytäjänsä Zucchinin mukaan.

ZUC tarttuu vain ohjelmatiedostoihin. Virus oli alunperin ohjelmoitu aktivoitumaan 2.3.1990 jälkeen. Puolitoista minuuttia käynnistyksen jälkeen tartunnan viruksen sisältämä ohjelma alkaa käyttäytyä oudosti. Kun hiiren näppäintä painetaan, kohdistin alkaa pomppia kuvaruudun reunasta toiseen. Virus on kuin Mac-versio PC:ssä tavattavasta Ping Pong-viruksesta, joka sekin on kotoisin Italiasta.

Joissakin Maceissä ZUC saattaa muuttaa työpöydän taustakuviointia ja hidastaa selvästi ohjelmien käynnistämistä. Muutoin virus on vaaraton. Se voi kuitenkin levitä lähiverkon kautta.

Useimmista muista viruksista poiketen ZUC ei muuta tartuttamansa tiedoston päiväystä.

Mac ja torjuntaohjelmat

Seuraavassa listassa on lueteltu eräitä Macille tarkoitettuja virusten torjunta- ja etsintäohjelmia. Koska virukset ovat yleisiä, on torjuntaohjelmiakin tehty melkoinen valikoima. Hyviä ohjelmia on useita, joten virusten havaitsemisen ajoissa ei pitäisi olla vaikeata.

AntiPan. Maksuton apuohjelma, joka etsii levyiltä nVIR-viruksia ja poistaa ne. Tunnistaa myös nVIRin eri muunnokset. Pystyy "rokottamaan" tiedostoja niin, ettei nVIR enää tartu niihin.

Disinfectant 1.8-versio tunnistaa kahdeksan erilaista Mac-virusta sekä niiden erilaiset variaatiot. Ohjelma pystyy myös parantamaan viruksen saastuttamat tiedostot takaisin kuntoon. Se toimii myös TOPS-verkossa. Toiminnan varmistamiseksi Disinfectant tarkistaa aina ennen käyttöä myös itsensä.

Interferon. Etsintäohjelma, joka huomaa sekä Scores- että nVIR-virukset. Haluttaessa ohjelma raportoi myös havaitsemistaan epäilyttävistä kohdista, jotka saattavat johtua viruksista. Interferon oli torjuntaohjelmien pioneeri Mac-maailmassa. Nykyisin sen käyttöä ei enää suositella, koska ohjelmassa on pieniä virheitä eikä se tunnista uusia viruksia. Tekijä onkin tehnyt ohjelmastaan uuden, kaupallisen Virex-nimisen version.

SAM. Etsintäohjelma, jonka voi asentaa monella tavoin. Haluttaessa se tarkistaa kaikki levykkeet heti, kun ne laitetaan levykeasemaan.Tarkistus voidaan tehdä myös aina koneen käynnistyksen tai sulkemisen yhteydessä tai erillisellä käskyllä. Toimii luotettavasti. Kaupallinen ohjelma, tekijänä Symantec.

VirusDetective. Hyvänä pidetty shareware-ohjelma, jonka käyttömaksu on 40 dollaria. Kun uusia viruksia löydetään, voidaan ohjelmaa laajentaa uusia viruksia vastaavaksi eikä uutta versiota tarvita. Havaitsee myös yleisimmät perusvirusten muunnokset.

Virus Rx. Applen oma, maksuton etsintäohjelma.Tunnistaa Scores-, nVIR-, INIT 29-, ANTI- ja WDEF-virukset, mutta ei pysty korjaamaan virusten saastuttamia ohjelmia.

6

Tunnettuja PC-viruksia

Tässä luvussa esitellään eräitä parhaiten tunnettuja PC-viruksia. Jokaisen viruksen kohdalla on kuvattu sen toiminta- ja lisääntymistavat. Yleisimpien virusten kohdalla on myös kerrottu menettely, jolla viruksesta pääsee eroon. Luvun lopussa on vielä esitelty lyhyesti joukko uusia ja/tai vähemmän tunnettuja viruksia.

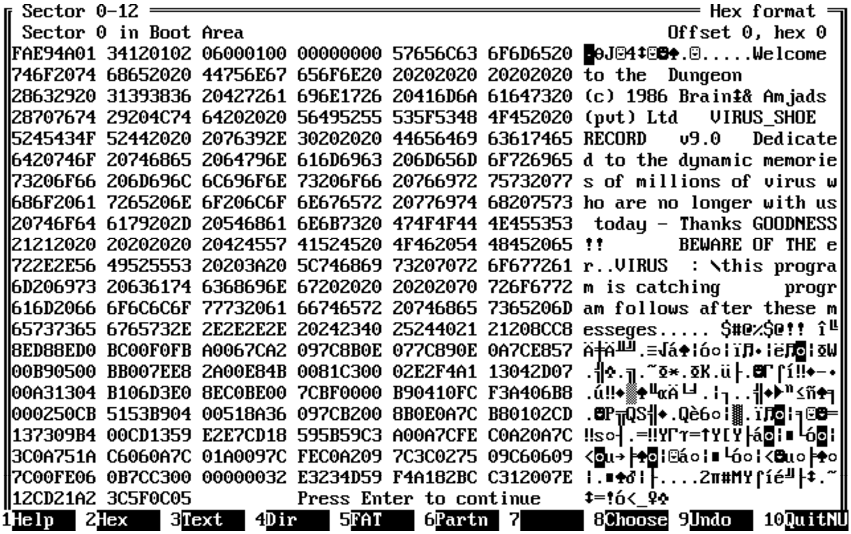
Virusten lista ei pyri olemaan täydellinen, eikä se voisikaan olla, sillä uusia viruksia syntyy koko ajan. Koska monista viruksista on liikkeellä useita hieman toisistaan poikkeavia versioita ja uusia tehdään koko ajan, saattavat virusten yksityiskohdat vaihdella.

Pakistanilainen

Nimiä	Brain, aivovirus, Basit-virus, Ashar
Tyyppi	levykevirus
Luokitus	lievästi vaarallinen

Kun Pakistanilainen tammikuussa 1986 havaittiin, se sai kunnian olla ensimmäinen löydetty PC-virus. Viruksesta on vuosien varrella kehitetty monia eri versioita ja sen arvellaan saastuttaneen yli 300000 levykettä.

Pakistanilais-viruksen alkuperästä liikkuu monia tarinoita ja uskomuksia. Totuuden selvittäminen näin monen vuoden jälkeen on lähes mahdotonta. Ainoa, mitä tiedetään varmuudella, ovat viruksen tekijät. Viruksen kirjoitti yhdessä veljensä Amjadin kanssa 19-vuotias Basit Alvi Lahoressa, Pakistanissa. He ikuistivat nimensä, osoitteensa ja



Brain-virus piiloutuu käynnistyslohkoon ja luo levykkeelle 3 kilotavun bad sector-alueen, johon alkuperäinen lohko ja loppuosa viruksesta tallennetaan. Kuva eräästä Brainin versiosta, jossa alkuperäisiä tekstejä on muutettu.

puhelinnumeronsa viruksen ohjelmakoodin keskelle selväkielisenä tekstinä. Teksti BRAIN COMPUTER SERVICES antaa ymmärtää, että viruksen nimi olisi tullut poikien yrityksen nimestä.

Uskottavimman tarinan mukaan veljekset myivät tekemäänsä laskentaohjelmaa. Laittoman kopioinnin estämiseksi he lisäsivät levykkeille Brain-rutiinin, joka aktivoitui tehdyistä kopioista. Joku tuntematon ohjelmoija meni kuitenkin muuttamaan koodia niin, että Brainista tuli virus.

Toisen tarinan mukaan veljekset myivät turisteille pilkkahintaan laittomia kopioita Lotuksen ja dBasen kaltaisista ohjelmista ja lisäsivät viruksen levykkeille rankaistakseen asiakkaitaan. Viruksessa olevia osoitetietoja ja tekstiä "Contact us for vaccination" on joskus erehdytty tulkitsemaan niin, että Brain olisi elektronista kiristystä.

Brain-virus tarttuu vain ja ainoastaan 360 kilon levykkeille. Se piiloutuu käynnistyslohkoon ja siirtää alkuperäisen lohkon samoin kuin osan itsestään perustamalleen 3 kilon bad sector-alueelle. Viruksessa

on laskuri, jonka täyttyessä se tartuttaa itsensä uudelle levykkeelle. Tekemällä tartunnan vain silloin tällöin se vähentää paljastumisen riskiä. Tarttumisen yhteydessä virus merkitsee levykkeen muuttamalla sen nimiöksi (c) Brain. Virus itse tunnistaa jo saastuttamansa levykkeet kuitenkin käynnistyslohkon neljännessä ja viidennessä tavuissa olevasta 1234-heksakoodista.

Alkuperäinen Brain-virus oli suhteellisen harmiton. Se saattoi tuottaa vahinkoa vain varatessaan levyltä 3 kilon bad sector -alueen. Viruksen käyttämä algoritmi ei ollut täydellinen ja varsinkin jos levyke oli lähes täysi, se varasi tilan olemassa olevien tiedostojen päälle pilaten näin niiden sisällön.

Viruksesta on vuosien aikana tehty useita muunnoksia. B-versiota on muutettu niin, että se pystyy tarttumaan myös kiintolevyille ("Houston virus"). Samalla sen sisältämiä tekstejä on muutettu. C-versiossa nimiön muuttava Brain-teksti on poistettu viruksen havaitsemisen vaikeuttamiseksi. Lisäksi viruksesta on liikkeellä versioita, joissa viruskoodissa olevia selväkielisiä tekstejä on peukaloitu ja eräs variaatio, joka sotkee FATin 5.5.1992 jälkeen käynnistettäessä. Ashar-versiossa (C) Brain teksti on korvattu tekstillä (C) Ashar.

Muistissa ollessaan Brain-virus pystyy hämäämään etsintä- ja tutkimisohjelmia. Virus varastaa levyn suoraan lukemiseen käytetyn keskeytyksen ja ohjaa sen osoittamaan omaa koodiaan. Jos keskeytystä käyttävä lukupyyntö kohdistuu käynnistyslohkoon, virus palauttaa bad sectoriin tallennetun alkuperäisen lohkon. Nortonin levytutkija tai virusten etsintäohjelma luulee, että levy on täysin kunnossa.

Brain-viruksen saastuttaman levykkeen tunnistaa helposti jo pelkällä DIR-käskyllä:

```
 Levy asemassa A on  (c) Brain .
 Hakemisto A:\

COMMAND  COM     25276 01.01.88    0.00
        1 tiedosto(a).Vapaana     279552 tavua.
```

CHKDSK-ohjelma näyttää levyllä olevien bad sectorien määräksi 3072 tavua:

```
Taltio  (c) Brain , luotu 00.00.1980 0.00.

    362496 tavua tilaa levyssä.
     54272 tavua 3 piilotiedostossa.
     25600 tavua 1 käyttäjätiedostossa.
      3072 tavua viallisissa sektoreissa.
    279552 tavua käytettävänä levyssä.

Kussakin varausyksikössä on       1024 tavua.
Levyssä on        354 varausyksikköä.
Levyssä on käytettävänä        273 varausyksikköä.

Kokonaismuistitila     655360 tavua.
    573104 tavua vapaana.
```

Varma merkki Pakistanilaisesta viruksesta on levykkeelle syntyvä nimi (C) Brain sekä 3072 tavun mittainen bad sector-alue.

Viruksen tuhoaminen

Koska virus tarttuu yleensä vain levykkeille, ei virusta kannata lähteä poistamaan. Kun saastuneilla levykkeillä olevat työtiedostot on kopioitu toisille levykkeille ja tiedostojen toimivuus tarkistettu, kannattaa saastuneet levykkeet heittää roskiin tai alustaa uudelleen. Jos virus on tarttunut kiintolevylle, sen voi poistaa käynnistämällä mikron alkuperäisellä DOS-levykkeellä ja kirjoittamalla SYS-ohjelmalla käynnistyslohko uudelleen. Tämä ei tuo bad sectoreiksi merkittyä tilaa uuteen käyttöön, mutta tuhoaa viruksen levyltä.

Jerusalem

Nimiä	PLO-virus, perjantai 13. päivä -virus, 1813-virus
Tyyppi	tiedostovirus
Luokitus	lievästi vaarallinen

Todennäköisesti PC-koneiden yleisin virus. Eristettiin ensimmäisen kerran Jerusalemin yliopistolla joulukuussa 1987. Virus tarttuu sekä

COM- että EXE-tiedostoihin, kasvattaen näiden pituutta vastaavasti 1813:lla ja 1808:lla tavulla. Virus ei tutki, onko EXE-tiedosto jo saanut tartunnan, vaan tarttuu siihen jokaisella ohjelman käynnistyskerralla uudelleen. Tartunnan saaneen tiedoston loppuun ilmestyy tunnus "sUMsDos" jota voi käyttää apuna virusta etsittäessä. Ei tartu COMMAND.COMiin.

Kun virus on ollut hieman vajaat 30 minuuttia muistissa, se tyhjentää kuvaruudun vasemmasta alareunasta 12 sarakkeen levyisen ja 2 rivin korkuisen alueen. Moni viruksen saaneista onkin luullut näyttökortin menneen rikki. Samalla koneen toiminta hidastuu, koska virus alkaa kiertää ylimääräisessä ja täysin turhassa silmukassa. Alkuperäisissä PC-koneissa hidastuminen on ollut niin suurta, ettei konetta ole voinut enää käyttää. Nopeat 286- ja 386-mikrot ajavat hidastussilmukankin niin nopeasti, ettei käyttäjä yleensä edes huomaa sitä.

Perjantaina, joka sattuu 13 päiväksi, virus poistaa kaikki ohjelmat joita käyttäjä yrittää ajaa. Ihmetellessään mitä oikein on tekeillä käyttäjä yrittää useiden eri ohjelmien ajamista, jolloin nekin katoavat. Eräs viruksen uhriksi joutunut käyttäjä kuvaili tilannetta kauheaksi, sillä "tiedostot katosivat silmiemme edessä".

Viruksesta tunnetaan useita hieman toisistaan poikkeavia versioita, joista yleisin on B-tyyppi. C-versiosta hidastussilmukka on poistettu. D-versiossa ohjelmien poistamiseen tarkoitettu koodi on korvattu osalla, joka sotkee levyn FATin. Espanjasta tavattu versio sisältää tekstin "ANARKIA" ja aktivoitumispäiväksi on muutettu tiistai 13. päivä. Uusi Jerusalemilainen ("New Jerusalem") on muuten tavallinen Jerusalem-virus, mutta koodia on muutettu etsintäohjelmien hämäämiseksi.

Marraskuussa Jerusalemilaisesta 1989 tavattiin muunnelma, joka poistaa käynnistettävät ohjelmatiedostot joka perjantai *paitsi* silloin kun se osuu 13. päiväksi. Virus sai nimen "Payday" (palkkapäivä). Yleisyytensä vuoksi Jerusalemilaista on myös käytetty kokonaan uusien virusten pohjana. Eräs näistä on Frere Jacques, joka soittaa perjantaisin nimikkosävelmäänsä (suomeksi Jaakko-kulta) koneen kaiuttimesta.

Jerusalemilaisen lisäksi on olemassa toiminnaltaan samanlainen, mutta paljon harvinaisempi virus, joka kulkee nimellä "Friday 13

COM". Virus eristettiin ensi kertaa Etelä-Afrikassa jo vuonna 1987. Virus ei ole muistinvarainen, vaan se tarttuu suoraan levyllä oleviin COM-ohjelmiin. Kun tartunnan saanut ohjelma käynnistetään, virus etsii levyltä kaksi puhdasta COM-ohjelmaa ja kirjoittaa itsensä niiden loppuun. Viruksen pituus on vain 512 tavua ja Jerusalemilaisen tapaan sen poistaa kaikki ohjelmat, joita yritetään ajaa perjantaina 13. päivä.

Viruksen tuhoaminen

Jerusalemilaisesta on helppo päästä eroon. Kone käynnistetään alkuperäisellä, kirjoitussuojatulla DOS-levykkeellä. Tartunnan saaneet ohjelmat etsitään jonkin luvussa seitsemän kuvatun apuohjelman avulla ja poistetaan levyltä.

Italialainen

Nimiä	Ping-Pong, Bouncing ball, Vera Cruz
Tyyppi	levykevirus
Luokitus	vaaraton

Kuten nimikin kertoo, viruksen uskotaan syntyneen Italiassa. Ensimmäiset havainnot siitä tehtiin maaliskuussa 1988. Viruksen uskotaan tulleen Suomeen Olivetin alkuperäisellä huoltolevykkeellä.

Osa viruksesta piiloutuu käynnistyslohkoon, osa levykkeelle luomaansa 1024 tavun mittaisen bad sectoriin. Keskimäärin 20 minuutin kuluttua virus tulostaa kuvaruudulle pienen pallon, joka muuttaa suuntaansa törmätessään ruudulla olevaan tekstiin tai näytön reunoihin. Pallo ei aiheuta vahinkoa eikä estä mikron käyttöä, mutta on vähintäänkin kiusallinen jos käyttäjä yrittää tehdä mikrolla työtään. Koneen sammuttaminenkaan ei auta, sillä pallo ilmestyy näkyviin pian sen jälkeen kun kone on käynnistetty uudelleen.

Viruksen tekijä on käyttänyt konekielistä käskyä MOV CX,AX joka toimii vain 8088-prosessorissa. Tästä syystä virus ei toimi koneissa, joissa on joko 286-, 386-, 486- tai V20-prosessori. Jos viruksen saastuttamaa käyttöjärjestelmälevykettä yritetään käyttää näissä koneissa

jää kone jumiin. Liikkeellä on tosin versio, jossa tämäkin rajoitus on korjattu. Viruksen B-versio tarttuu myös kiintolevylle. Joissakin tapauksissa virus saattaa merkitä bad sectorin vain toiseen kahdesta FATista mikä voi myöhemmin johtaa ongelmiin levyä käytettäessä.

Viruksesta on tehty myös aivan toisenlainen versio ("Typo"), jossa virus palloefektin sijaan sotkee kirjoittimelle menevän tekstin.

Viruksen tuhoaminen

Kone käynnistetään puhtaaksi tiedetyllä ja kirjoitussuojatulla DOS-levykkeellä. Tämän jälkeen tartunnan saaneet levykkeet on helppo tunnistaa niillä olevasta 1024 tavun bad sector-merkistä. Ellei levykettä välttämättä tarvita, kannattaa saastuneet levykkeet tuhota tai alustaa uudelleen. Tärkeät levykkeet voi parantaa antamalla komento C>SYS A: joka kirjoittaa levykkeelle uuden käynnistyslohkon ja tuhoaa siinä olleen viruksen. Bad sectorilla merkittyä kilotavun mittaista aluetta tämä ei kuitenkaan tuo käyttöön.

Yankee doodle

Tyyppi	tiedostovirus
Luokitus	vaaraton

Todennäköisesti Länsi-Saksassa tai Bulgariassa kehitetty virus, joka tarttuu sekä COM- että EXE-tiedostoihin ja soittaa silloin tällöin, yleensä tasan kello 17, muutaman tahdin nimikkosävelmästään. Ohjelman pituus kasvaa 2881..2897 tavulla. Viruksesta on useita eri versioita ja versionumero on merkitty viruksen koodiin.

Yankee Doodle on harmiton: se ei poista tiedostoja eikä aiheuta vahinkoa käyttäjälle.

Muuan hämmästyttävä piirre tässä viruksessa on se, että kun viruksen saastuttamaa ohjelmaa tutkitaan saastuneella DEBUGilla, virus *poistuu* ohjelmasta ja tiedoston pituus palautuu takaisin alkuperäiseen arvoonsa.

Versiosta 44 alkaen virus muuntaa löytämänsä Italialaisviruksen niin, että se tuhoaa itse itsenä 256:n käynnistyksen jälkeen. Uudemmissa versioissa virus muuntaa myös löytämäänsä 1701-virusta. Alkuperäinen perus-Yankee Doodle ("Old Yankee", joskus myös nimellä "Yankee Doodle-2") tarttuu vain EXE-tiedostoihin kasvattaen niiden pituutta 1961 tavulla. Se ei jää keskusmuistiin vaan etsii uhrinsa suoraan levyltä kun viruksen saastuttama ohjelma käynnistetään. Musiikki kuuluu aina kun virus onnistuu tarttumaan uuteen ohjelmaan.

Yankee Doodlella on paljon yhteistä Vacsina-viruksen kanssa. Todennäköisesti virukset ovat kotoisin samasta lähteestä.

Viruksen tuhoaminen

Kone käynnistetään puhtaaksi tiedetyllä ja kirjoitussuojatulla DOS-levykkeellä. Saastuneet tiedostot paikallistetaan etsintäohjelman avulla ja poistetaan. Jos virus on tarttunut johonkin tärkeään ohjelmatiedostoon, josta ei ole puhdasta varmuuskopiota, voi virusta yrittää poistaa DEBUGin avulla. Temppu ei silti välttämättä toimi kaikkien versioiden kohdalla.

Vacsina

Tyyppi	tiedostovirus
Luokitus	vaaraton

Länsi-Saksasta peräisin oleva virus, joka tarttuu ohjelmatiedostoihin ja kasvattaa niiden pituutta 1206..1218 (COM) tai 1346..1350 (EXE) tavulla. Tarttumismekanismi on muutenkin erikoinen, sillä koneen kaiutin piippaa merkiksi tartunnan tapahtumisesta. EXE-tiedostojen tartuttaminen tapahtuu kahdessa vaiheessa. Ensimmäisessä vaiheessa EXE-tiedosto valmistellaan niin, että virus pystyy tarttumaan siihen ja varsinainen tartuttaminen tapahtuu vasta toisella käynnistyskerralla. Molemmat vaiheet kasvattavat pituutta mutta piippaus kuullaan vasta jälkimmäisellä kerralla. Muista viruksista poiketen Vacsina muuttaa tiedoston päiväyksen tartuntahetken tilannetta vastaavaksi. Muuttuneita

päiväyksiä seuraamalla voi onnistua jäljittämään viruksen kulkureitin omaan koneeseen.

Jos virus huomaa, että ohjelmassa on sen vanhempi versio, se korvaa tämän uudemmalla. Viruksessa on siis automaattinen päivitysmekanismi. Viruksesta on liikkeellä useita eri versioita.

Vacsina ei vähennä muistin kokonaismäärää. Vapaa keskusmuisti vähenee kuitenkin 1216 tavulla.

Viruksen tuhoaminen

Kone käynnistetään puhtaaksi tiedetyllä ja kirjoitussuojatulla DOS-levykkeellä. Saastuneet tiedostot paikallistetaan etsintäohjelman avulla ja poistetaan.

Dark Avenger

Laite	DOS
Tyyppi	tiedostovirus
Luokitus	erittäin vaarallinen

Dark Avenger-virus on erittäin tarttuva ja vahingollinen virus. Se tarttuu COM- ja EXE-tiedostoihin kasvattaen niiden pituutta 1800 tavulla. Viruksen sisältä löytyvät tekstit "Eddie lives...somewhere in time", "Diana P." ja "This program was written in the city of Sofia (C) 1988-1989 Dark Avenger". Viruksesta on liikkeellä myös versio jossa tekstit on korvattu pelkillä välilyönneillä.

Muista viruksista poiketen tämän syntyhistoria tunnetaan hyvinkin tarkkaan. Viruksen tehnyt bulgarialainen on salanimeä "Krad Regneva" (viruksen nimi takaperin kirjoitettuna) käyttäen jakanut auliisti tietoja viruksestaan ja levitellyt jopa viruksensa listausta rohkaisten muita tekemään sen pohjalta uusia viruksia. Tällainen vastuuttomuus hakee vertaistaan jopa tietokonerikollisuuden piirissä!

Tekijä kertoo aloittaneensa viruksen koodaamisen syyskuussa 1988 ja olleensa siten ensimmäinen bulgarialainen viruksentekijä. Levinnein (muttei tehokkain eikä varmasti viimeinen) lienee viruksen 1.31-versio,

joka valmistui ja lähetettiin liikkeelle 3. tammikuuta 1989. Kuin anteeksipyyntönä tekijä on myös laittanut levitykseen DOCTOR-nimisen ohjelman, jolla virus voidaan poistaa tartunnan saaneista ohjelmista.

Kun viruksen sisältävä ohjelma käynnistetään, virus varaa koko keskusmuistin itselleen ja pakottaa ohjelman päätyttyä käyttöjärjestelmän lataamaan komentotulkin uudelleen muistiin. Näin virus tarttuu heti myös COMMAND.COMiin, vaikka se olisi alihakemistossakin.

Dark Avenger on tehty pirullisen nerokkaasti. Se pystyy huijaamaan useimpia muistinvaraisia torjunta- ja suojausohjelmia ja se leviää erittäin nopeasti. Viruksen ollessa muistissa riittää komento

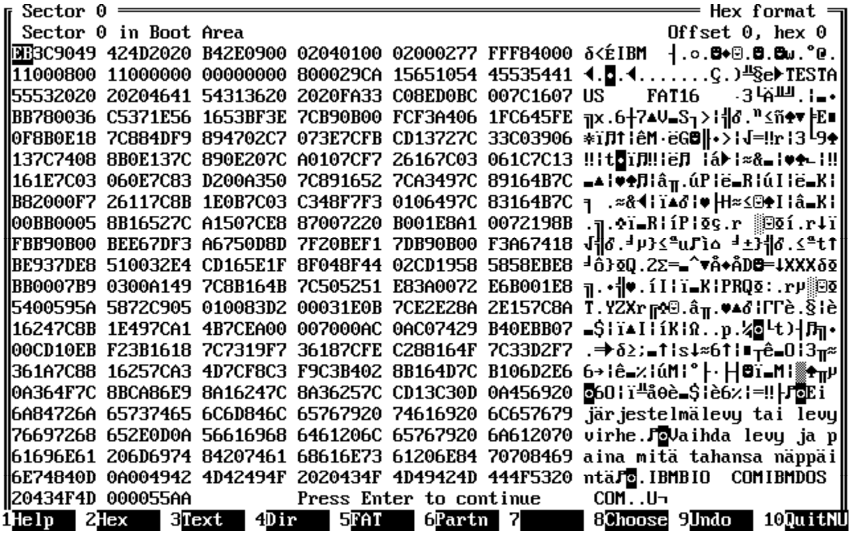
```
C>COPY A:SOFTA.EXE C:
```

tartuttamaan viruksen sekä alkuperäiseen tiedostoon A: levykkeelle että siitä C: asemalle tehtävään kopioon.

Virusten etsimiseen ja tarkistussummien laskemiseen käytetyt ohjelmat joutuvat avaamaan jokaisen levyllä olevista ohjelmista lukiessaan sen läpi. Tämä lukuvaihe riittää viruksen tartuttamiseen. Kunnolla tehdyn etsintäohjelman pitäisikin varmistua siitä, ettei Dark Avenger tai mikään muu samaan tapaan toimiva virus ole muistissa ennen kuin tiedostojen lukeminen aloitetaan.

Aina, kun viruksen saastuttama ohjelma käynnistetään, Dark Avenger käy kasvattamassa laskuria, joka sijaitsee levyn käynnistyslohkossa. Laskuri on sijoitettu lohkon alkuun, jossa normaalisti on levyn alustamiseen käytetyn DOSin tunnus (esimerkiksi IBM 4.0 jos alustus on tehty IBM:n PC-DOS 4.0-versiolla). Viruksen voikin havaita siitä, että tunnuksen nimi on oikein, mutta numeroiden paikalla näkyy puoligraafisia tai muuten mahdottomia merkkejä.

Laskuria apuna käyttäen Dark Avenger käy kirjoittamassa suoraan kiintolevylle osan omasta koodistaan (mm. juuri tekstin "Eddie lives"). Jos kohdalla sattuu olemaan ohjelmakoodia, ei ohjelma enää tämän jälkeen toimi. Vielä ikävämmin käy työtiedostolle. Ellei kyseessä ole pelkkä tekstitiedosto vaan esimerkiksi taulukkolaskennan malli, ei alkuperäinen sovellus enää pysty käsittelemään sitä. Koska tiedostoille tapahtuva vahinko ei näy ulospäin, ei käyttäjä yleensä huomaa mitä on



Dark Avenger käyttää levyn käynnistyslohkoa työtilanaan. DOS-tunnuksen perässä olevat numerot muuttuvat puoligraafisiksi merkeiksi kun Dark Avenger kirjoittaa niiden päälle. Tätä voi käyttää apuna viruksen paljastamisessa.

tekeillä. Käyttäjä saattaa jopa tehdä hyvässä uskossa varmuuskopioita pilaantuneista tiedostoista. Kun vahinko selviää, on jo liian myöhäistä pelastaa ainakaan kaikkia tiedostoja.

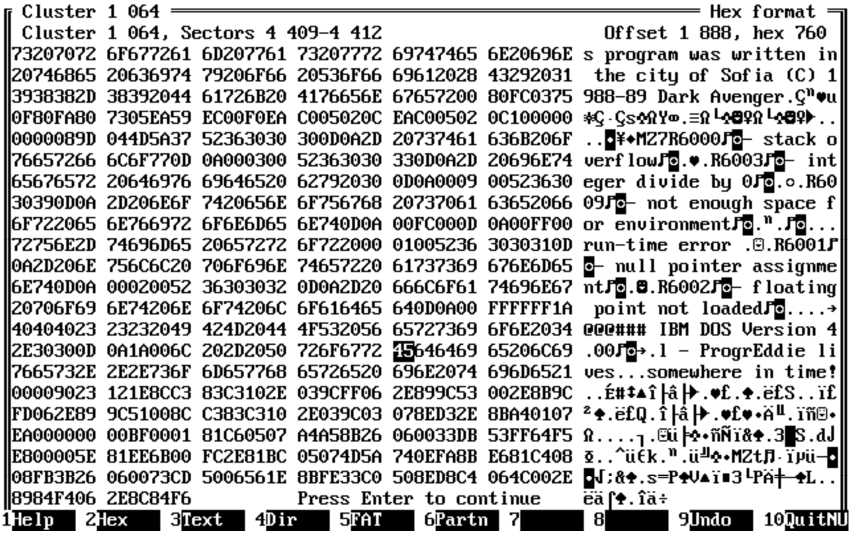
Viruksen voi havaita ajoissa tutkimalla käynnistyslohkon DOS-tunnusta tai tarkkailemalla keskusmuistin määrää. Se putoaa viruksen myötä 651664:ään tavuun, josta vapaan tilan vähenemiseksi jää 3696 tavua. Viruksen voi joskus havaita myös alihakemiston nimien sekoamisena. Sekoaminen johtuu siitä, että alihakemistot on sijoitettu levyllä sinne tänne normaalien tiedostojen tapaan ja jos Dark Avengerin tekemä kirjoitus sattuu osumaan keskelle hakemistoa, näkyy se virheinä hakemistojen nimitiedoissa. Tällaiset virheet paljastuvat myös CHKDSKillä, koska se tarkistaa FATin lisäksi hakemistorakenteen oikeellisuuden.

Dark Avengerin lähdekielinen, tekijänsä kommentein varustettu ohjelmalistaus on kiertänyt maailmalla ja houkutellut muita ohjelmoijia. Eräs Dark Avengerin pohjalta tehdyistä viruksista kulkee nimellä

V2000. Joskus sitä kutsutaankin Dark Avenger II:ksi. Esikuvansa tapaan se tuhoaa kiintolevyn tiedostoja kirjoittamalla joka 16 käynnistyskerralla satunnaiseen kohtaan levyä kopion käynnistyssektorista. Viruksesta on liikkeellä useita versioita. Joidenkin sisältä löytyy teksti "Only the Good die young..." ja toisista "Copy me - I want to travel". Virus kasvattaa tartuttamansa tiedoston pituutta 2000 tavulla. Viruksen sisältä löytyy myös teksti "(C) 1989 by Vesselin Bontchev". Mainittu henkilö on Bulgarian tunnetuin virustenmetsästäjä. Onkin todennäköistä, että viruksen tekijä on halunnut näin mustata hänen mainettansa - tai sitten Bonchev viettää pahimman laatuista kaksoiselämää.

Viruksen tuhoaminen

Jos Dark Avenger löytyy omasta koneesta ovat hyvät neuvot tarpeen. Kone on välittömästi suljettava ja käynnistettävä alkuperäisellä kirjoitussuojatulla DOS-levykkeellä. Työtiedostot on varmistettava uusille,



Dark Avenger on erityisen vaarallinen siksi, että se kirjoittaa omaa koodiaan suoraan levylle. Alle jäävät tiedostot, ovatpa ne sitten ohjelma- tai työtiedostoja, muuttuvat käyttökelvottomiksi. Levylle kirjoitettavasta osasta käy ilmi, että virus on peräisin Bulgariasta.

toisessa koneessa alustetuille levykkeille. Vanhoja varmistuksia ei missään tapauksessa pidä tuhota, sillä ainakin osa kiintolevyn työtiedostoista on todennäköisesti käyttökelvottomia. Viimeksi varmistettujen työtiedostojen toimivuus on testattava yksi kerrallaan ja tarvittaessa käytettävä vanhaa, toivottavasti kunnossa olevaa varmistusta. Virus pääsee erittäin helposti takaisin kiintolevylle, joten puhdistautuminen on tehtävä tavallistakin huolellisemmin.

Disk Killer

Nimiä	Ogre, Computer Ogre
Tyyppi	levykevirus
Luokitus	erittäin vaarallinen

Disk Killer on monessa suhteessa poikkeuksellinen virus. Se on teknisesti varsin kehittynyt ja kooltaan suhteellisen iso. Aktivoituessaan se tulostaa ruudulle näyttävän ilmoituksen, josta kuka tahansa käyttäjä tajuaa joutuneensa viruksen uhriksi.Disk Killer olikin eräs ensimmäisistä Suomessa havaituista viruksista. Ensimmäinen havainto siitä tehtiin alkusyksyllä 1989, jolloin virus oli vielä maailmallakin lähes tuntematon.

Disk Killer piiloutuu levykkeellä käynnistyslohkoon ja tekemäänsä bad sectoriin, jonka koko on 1,2 megan lerpulla 5120 tavua ja 360 lerpulla 6144 tavua. Viruksessa on ohjelmointivirhe, jonka vuoksi se joskus kopioi itsensä keskelle levyä ja merkitsee väärän kohdan bad sectoriksi. Kiintolevylle päästyään virus piilottaa bad sector-osuuden nollauran sektoreihin 13-17.

Virus pyrkii kopioimaan itsensä jokaiselle 5,25" levykkeelle, jota järjestelmässä käytetään. Pelkkä DIR A: riittää tartuttamaan viruksen A: asemassa olevalle levykkeelle. Korppuihin virus ei osaa tarttua ja pelkkä yrityskin tuottaa virheilmoituksen.

Satunnaisen ajan kuluttua, joka yleensä vaihtelee muutamasta viikosta muutamaan kuukauteen, virus äkkiä aktivoituu. Ruudun sisältö tyhjenee ja sille tulostuu teksti:

```
     Disk Killer -- Version 1.00 by COMPUTER OGRE 04/01/1989

                          PROCESSING




                           WARNING!!

Don't turn off the power or remove the diskette while Disk Killer
                        is Processing!
```

PROCESSING-ilmoitus näkyy vilkkuvalla punaisella ja alimman rivin teksti käänteisellä taustalla. Computer Ogre tarkoittaa tietokone-örkkiä ja ruudun oikeassa ylänurkassa näkyy aprillipäivän päiväys.

Tekstin näkyessä ruudulla virus tuhoaa kiintolevyn siten, että se koodaa uloimmat urat suorittamalla tavuille XORin vuorotellen arvojen AAAA ja 5555 kanssa. Käsittely saattaa viedä melkoisesti aikaa. Kun se on päättynyt, tulostuu ruudulle vielä teksti "I wish you luck!"

Jos virus iskee, saattaa nopea toiminta pelastaa osan tiedostoista. Tärkeimmät uloimmat raidat on kuitenkin sotkettu hyvin nopeasti, jolloin levyn osiotaulukko ja kirjanpito ovat menneet. Käsittelyn jälkeen mikro ei löydä kiintolevyä enää lainkaan. Ainoa tapa saada levy jälleen käyttöön on jakaa se FDISKin avulla uudelleen osioihin, alustaa jokainen osio FORMATilla ja yrittää sen jälkeen pelastaa ylikirjoittamiselta välttyneitä tiedostoja varausyksikkö kerrallaan. Käytännössä työ on suurin piirtein toivotonta.

Periaatteessa olisi myös mahdollista suorittaa toinen XOR-käsittely, joka kumoaisi ensimmäisen vaikutuksen ja palauttaisi jälleen levyn ennalleen. Käsityönä sitä ei kuitenkaan kannata lähteä yrittämään.

Viruksen tuhoaminen

Jos virus havaitaan ajoissa, on kone käynnistettävä puhtaalla ja suojatulla DOS-levykkeellä. Kiintolevyn käynnistyslohkossa oleva osa viruksesta tuhotaan siirtämällä käyttöjärjestelmä uudelleen komennolla

A> SYS C:. Vaarattomaksi muuttunut osa viruksen koodista jää kuitenkin nollauralle ja sen puhdistaminen onnistuu vain jonkin apuohjelman avulla (CLEAN, Norton, yms.)

Viruksen saastuttamat levykkeet voi tunnistaa bad sectorien määrästä. Levykkeillä osa viruksesta sijaitsee todennäköisesti jonkin tiedoston päällä, joten tiedostojen kunto pitää tarkistaa ennen kuin niitä yritetään käyttää. Tarkistuksen jälkeen on saastuneet levykkeet varminta tuhota tai alustaa uudelleen.

Stoned

Nimiä	Uusi-Seelantilainen, Marijuana, San Diego, Hawaii
Tyyppi	levykevirus
Luokitus	vaaraton

Stoned-viruksen uskotaan syntyneen vuoden 1988 alussa Uudessa Seelannissa. Alunperin virus tarttui todennäköisesti vain 5,25" levykkeille, mutta joku on muokannut sitä matkan varrella niin, että virus tarttuu nykyisin myös kiintolevyille.

Levykkeellä Stoned-virus piiloutuu käynnistyslohkoon, mutta sijoittaa osan itsestään päähakemiston loppuun. 360 kilon levykkeellä voi olla enintään 96 tiedostonimeä jotta virukselle jäisi riittävästi tilaa. Erilaisesta rakenteestaan johtuen riittää 1,2 megatavun lerpulla jo 49. tiedostonimi kirjoittamaan viruksen koodin päälle ja tuhoamaan sen. Kiintolevyllä Stoned-virus kopioi alkuperäisen osiotaulukon ja siihen liittyvän latausohjelman seitsemänteen sektoriin ja sijoittaa itsensä osiotaulukon paikalle ensimmäiseen sektoriin.

Virus on toiminnaltaan varsin harmiton. Noin joka kahdeksannella käynnistyskerralla se tulostaa ruudulle ilmoituksen "Your PC is now Stoned! LEAGALISE MARIJUANA" (Suomeksi: PC:si on pilvessä. Marijuana lailliseksi!) Eräissä versioissa jälkimmäinen ilmoitus saattaa jäädä näkymättä ja ensimmäinenkin ilmoitus tulostuu vain levykekäynnistyksessä. Viruksen C-versio ei näytä mitään tekstiä, joten sen havaitseminen on vaikeata. Tuorein versio on D, joka osaa tarttua myös 3,5" korpuille.

Virus ei aiheuta vahinkoa. RLL-kiintolevyohjaimet saattavat tosin jäädä jumiin käynnistyksen yhteydessä ja muitakin yhteensopivuusongelmia saattaa ilmetä.

Viruksen tuhoaminen

Viruksen poistaminen kiintolevyltä on erittäin hankalaa, koska alkuperäinen osiotaulukko pitäisi siirtää takaisin ensimmäiseen sektoriin ja nollaura puhdistaa. Työ kannattaa jättää erityisen virusten poistamiseen tarkoitetun apuohjelman hoidettavaksi. Pelkkä kiintolevyn uudelleen alustaminen ei tuhoa virusta, koska FORMAT-ohjelma ei puhdista nollauraa eikä kirjoita osiotaulukkoa uudelleen. Levykkeiltä viruksen voi poistaa siirtämällä käyttöjärjestelmän uudelleen SYS-ohjelmalla. Ellei levykkeellä ole käyttöjärjestelmää, on levyke viisainta hävittää tai alustaa uudelleen sen jälkeen kun sillä olleet tiedostot on kopioitu turvaan.

1701 / 1704

Nimiä	Cascade, Fall, Falling letters, Drip, Melt
Tyyppi	tiedostovirus
Luokitus	vaaraton

17XX-virukset muodostavat kokonaisen virusperheen, jonka jäsenet poikkeavat vain hieman toisistaan. Virus on Jerusalemilaisen ohella Suomen yleisin virus. Sen juuret ovat vanhassa troijalaisessa ohjelmassa, jonka piti kytkeä Num Lock-valo pois päältä käynnistyksen yhteydessä, mutta joka sen sijaan pudottikin osan kuvaruudulla näkyvistä kirjaimista alimmalle riville. Tuntematon ohjelmoija teki ohjelmasta virusversion ja levitti sen niin hyvin, että viruksesta tunnetaan nykyisin useita eri versiota ja se on levinnyt hyvin laajalle. Viruksen nimi tulee määrästä, jolla saastuneen COM-tiedoston koko kasvaa. Virus ei tartu EXE-tiedostoihin.

Alkuperäinen virus aktivoitui satunnaisesti vuosina 1980 ja 1988 ja silloinkin vain 1.10. - 31.12. välisenä aikana, mistä viruksen syksyn

```
D:\WI >dir  W
     N     /
 Volume in drive D is D ASEMA
 Dire tory  f   D:\WIN

.         o    ..               DESIGNER        EXCEL           PM3
ABC       TXT  CALC      EXE    CALENDAR EXE    CARDFILE EXE    CLIPBRD  EXE
CLOCKc    EXE  CONTROL   EXE    COURB    FON    COURC    FON    COURD    FON
CVTPAINT  EXE  KOE       MSP    DOSKOMEN DOC    DESKJET  DRV    DOSKOMEN WRI
DOTHIS    TXT  HELVB     FON    HELVC    FON    HELVD    FON    HIMEM    SYS
XER4020   DRV  WIN       INI    KUOPIO   WRI    MEMSET   EXE    MGXPS    DRV
MODER     FON  MSDOS     EXE    NOTEPAD  EXE    OSTA ENE WRI    PAINT    EXE
PIFED T   EXE  PRACTICE  WRI    README   TXT    REMMV    SYS    REVERSI  EXE
ROMANN    FON  SCRIPT    FON    SMARTDRV SYS    SPOOLER  EXE    TERMINAL EXE
TMSRBI    FON  TMSRC     FON    TMSR     FON    TUKIB    WRI    PSCRIPT  DRV
VERKK     WRI  READMEPS  TXT    WIN D    COM    WIN200   BIN    WIN200   OVL
WINOLOAP  GRB  WINOLDAP  MOD    WRITE    EXE    WIN87EM  EXE    COMMAND  PIF
SNAP      EX   HDCLIB    EXE    COLOR    EXE    LASS T     I    RAMD  VE S S
A4TRA     T E  WIN       OLD     SLP 2   DJ      OR             TEKO
TELE       X   SUTTU     WRI    F   T
     D 72   le(s)    909312 byte  fr e

D:\WIY>    T
     N    Fi                    s   e           W  DY    WR          RI    Y
```

1701/1704-virus aktivoituu syksyllä ja pudottaa silloin ruudulla näkyviä kirjaimia alaspäin. Tästä virus on saanut lempinimen "syksyn lehdet".

lehtiin viittaava nimikin on peräisin. 1701-B pudottaa kirjaimet vuodesta riippumatta. Versiot, jotka kasvattavat tiedostojen pituutta 1701:llä tavulla toimivat kaikissa mikroissa. Kolme tavua pidempi 1704-versio ei tartu koneisiin, joiden BIOSissa lukee IBM. Eräät versiot (Cascade-B) aiheuttavat kirjainten putoamisen sijasta alkulatauksen (reboot) ja 1701-Format versio kiintolevyn alustamisen. Virus itse on koodattu niin, ettei sitä voi tutkia suoraan levyltä lukemalla.

Viruksen tuhoaminen

Kone käynnistetään puhtaaksi tiedetyllä ja kirjoitussuojatulla DOS-levykkeellä. Saastuneet tiedostot paikallistetaan etsintäohjelman avulla ja poistetaan.

Alabama

Tyyppi	tiedostovirus
Luokitus	lievästi vaarallinen

Alabama-virus löydettiin Jerusalemin yliopistosta lokakuussa 1989. Se tarttuu EXE-tiedostoihin ja kasvattaa niiden pituutta 1560 tavulla.

Kun virus on ollut tunnin muistissa, se tulostaa ruudulle ilmoituksen "SOFTWARE COPIES PROHIBITED BY INTERNATIONAL LAW....... Box 1055 Tuscambia ALABAMA USA." Virus ei tartu ohjelmaan, joka käynnistetään, vaan etsii käynnistyksen aikana levyltä jonkin muun ohjelman ja tarttuu siihen. Vasta sitten kun hakemistosta ei löydy yhtään puhdasta tiedostoa, virus tarttuu käynnistettävään ohjelmaan. Perjantaisin ajettuna se käy vaihtamassa levyn kirjanpidossa olevia tietoja niin, että ajettavan ja saastutettavaksi valitun tiedostojen paikat vaihdetaan.

Alameda

Nimiä	Yale, Peking, Merritt, Sacramento, Golden Gate
Tyyppi	levykevirus
Luokitus	lievästi vaarallinen

Alameda-nimi tulee californialaisesta Alameda Collegesta, josta virus ensiksi havaittiin vuonna 1987.

Alkuperäinen virus tarttui vain 360 kiloisten levykkeiden käynnistyslohkoon ja sijoitti loput koodistaan levykkeen viimeiseen lohkoon (ura 39, puoli 0, sektori 8), jolloin alle mahdollisesti jäänyt tiedosto tuhoutui. Alkuperäinen virus käytti POP CS-konekielikäskyä, joten se pystyi toimimaan vain 8088- tai 8086-prosessoreissa. Uudemmissa viruksen versioissa (Sacramento-virus) tämä on korjattu. Alkuperäinen virus sisälsi laskurin, mutta ei koskaan tehnyt mitään. Se levisi A: asemassa olevalle levykkeelle kun käyttäjä painoi CTRL-ALT-DELiä haluten käynnistää koneen uudella levykkeellä. Viruksen C-versio (kulkee myös nimellä "SF virus") sotkee levykkeen laskurin edettyä 100 asti.

Viruksen Golden Gate-versio alustaa kiintolevyn laskurin tullessa täyteen. Raja-arvona on 500 tartutettua levykettä, joten sen täyttyminen kestää useita vuosia. Laskuri alkaa nollasta jokaisella uudella viruksen saastuttamalla levykkeellä. Vahingontekoa on nopeutettu B-versiossa vähentämällä laskurin raja-arvo 30:een.

Vaikka virus onkin jo vanha, se on hyvin harvinainen.

Lehigh

Tyyppi	erikoistunut tiedostovirus
Luokitus	erittäin vaarallinen

Lehigh-virus on saanut nimensä Lehigh-yliopistosta, josta se löydettiin marraskuun lopulla 1987.

Lehigh-virus on hyvin erikoistunut: se tarttuu vain COMMAND. COMiin. Virus kirjoittaa itsensä ohjelman sisällä olevalle noin 300 tavun mittaiselle pinoalueelle, joten COMMAND.COMin pituus ei muutu. Kun virus on muistissa ja asemaan laitetaan levyke, virus käy tarkistamassa sen. Jos levykkeeltä löytyy COMMAND.COM, virus kirjoittaa itsensä siihen. Viruksen tartuttaminen tapahtuu DOSin omia komentoja käyttäen. Tämän vuoksi COMMAND.COMin päiväys muuttuu ja jos tiedosto tai levyke on suojattu, tulostuu virheilmoitus.

Viruksen sisällä on laskuri, joka neljään ehdittyään aloittaa vahingonteon. Tällöin virus kirjoittaa 32 ensimmäistä lohkoa täyteen suttua mikä riittää tuhoamaan levyn kirjanpidon ja osan tiedostoista. Koska neljä kopiota on tehty varsin nopeasti, ei virus ehtinyt levitä kovinkaan laajalle koulun ulkopuolelle.

Viruksen 2-versio löydettiin samasta yliopistosta 2.2.1989. Tämä versio sotkee levyn 10:n tartuntakerran jälkeen. Parantuneen valvonnan vuoksi se ei ehtinyt levitä edes niinkään laajalle kuin edeltäjänsä.

Viruksen tuhoaminen

Koska virus tarttuu vain komentotulkkiin, se on helppo tuhota. Kone käynnistetään puhtaalla DOS-levykkeellä. Sillä oleva COMMAND.

COM kopioidaan kiintolevyllä ja levykkeillä olevien komentotulkkien päälle. Tulkin on kuitenkin oltava samaa versionumeroa kuin mitä levyllä oleva, viruksen saastuttama tulkki. Ellei näin ole, alkulataus keskeytyy DOSin antamaan virheilmoitukseen.

Islantilainen

Nimiä	One in Ten, 656, Saratoga
Tyyppi	tiedostovirus (EXE)
Luokitus	vaaraton

Islantilaisviruksen tapaus osoittaa, etteivät pohjoismaatkaan ole jääneet virusten kehittelyssä paitsioon. Alkuperäinen Islantilaisvirus havaittiin kesäkuussa 1989. Se tarttuu vain EXE-tiedostoihin kasvattaen niiden pituutta 656-671 tavulla. Tartunnan jälkeen tiedoston pituus on aina jaollinen 16:lla.

Muistissa ollessaan virus tarttuu joka 10. ajettavaan ohjelmaan. Jos koneen kiintolevy on vähintään 20 megatavua, se merkitsee jokaisen tarttumiskerran aikana yhden vapaan varausyksikön bad sector-merkillä. Vika-alueiden määrän kasvu helpottaa viruksen löytämistä.

Viruksen II-versio löydettiin kuukautta alkuperäisen jälkeen. Viruksen toiminta on I-version kaltainen, mutta sen teknistä rakennetta on muutettu torjuntaohjelmien hämäämiseksi.

III-versio löydettiin joulukuussa 1989. Viruksen rakennetta on jälleen paranneltu mikä on johtanut viruksen koon kasvuun. Saastunut tiedosto kasvaa 848-863 tavulla. Joulukuun 24 päivä ajettuna virus tulostaa ruudulle tekstin "Gledileg jol" ("hauskaa joulua" islanniksi).

Islantilaista virusta on todennäköisesti käytetty pohjana myös MIX-viruksessa, joka löydettiin Israelista elokuussa 1989. Virus tarttuu EXE-ohjelmiin kasvattaen niiden kokoa 1618-1634 tavulla. Alle 8 kilon ohjelmat jätetään rauhaan. Virus sotkee sekä sarja- että rinnakkaisliitäntään menevän tulostuksen ja pitää Num Lock-valoa jatkuvasti päällä.

Fu Manchu

Tyyppi tiedostovirus
Luokitus vaaraton

FuManchu-virus on etäistä sukua Jerusalemilaiselle. Joku ohjelmoija on ottanut Jerusalemin, purkanut sen osiinsa ja koonnut niistä aivan eri tavalla käyttäytyvän viruksen. Virus tarttuu COM-tiedostojen alkuun kasvattaen niiden pituutta 2080:lla tavulla, mutta jättää COMMAND. COMin rauhaan. EXE-tiedostoissa virus tarttuu ohjelman loppuun, jolloin pituus kasvaa 2086:lla tavulla. Viruksen eriskummallinen nimi tulee ohjelmakoodissa olevista kirjaimista "sAXrEMHOr", joista saadaan Sax Rohmer - Fu Manchun kirjoittaja.

Kun virus on muistissa ja käyttäjä painaa CTRL-ALT-DEL, virus tulostaa ruudulle hitaasti tekstin "The world will hear from me again" ja suorittaa uudelleenkäynnistyksen vasta tämän jälkeen.

Viruksen tekijällä on ollut erikoinen huumorintaju. Virus nimittäin tarkkailee näppäimistöä ja aina kun se huomaa sanat Thatcher, Reagan, Botha, Waldheim tai Fu Manchu, se lisää jotain tekstiä niiden perään ("Botha is a bastard", "Waldheim is a Nazi", "Thatcher is a cunt", "Reagan is a arshole"). Oman nimensä perään se kirjoittaa "3/10/88 - latest in the new fun line!" Tämä osa viruksesta aktivoituu vain elokuun 1989 jälkeen. Nimet ja sanat on koodattu, joten niitä ei voi käyttää viruksen etsimiseen. Reaganin perään tulostuvasta tekstistä voi päätellä, ettei tekijän englanninkielentaito ole ollut hänen ohjelmointitaitonsa veroinen.

Traceback

Tyyppi tiedostovirus
Luokitus vaaraton

Traceback-virus on kaukaista sukua 1701-virukselle. Virus on kooltaan poikkeuksellisen suuri: tartunnan saaneiden COM- ja EXE-tiedostojen koko kasvaa peräti 3066 tavulla. Virus tarttuu sekä käynnistettävään ohjelmaan että yhteen muuhun ohjelmaan, jonka virus etsii levyltä.

Virus ei tee varsinaista vahinkoa, mutta saattaa joissain tapauksissa kaataa koneen.

Virus on saanut nimensä tavasta, jolla se leviää. Tartunnan saaneeseen tiedostoon tallentuu tartuttajatiedoston nimi, mikä mahdollistaa viruksen jäljittämisen. Virus pitää myös yllä laskuria, joka kertoo montako tiedostoa se on tartuttanut.

28.12.88 jälkeen virus esittää kerran tunnissa tempun, jossa se pudottaa ruudulla näkyvät kirjaimet näytön alariville ja palauttaa ne minuutin jälkeen takaisin oikeille paikoilleen, ikään kuin muistona alkuperästään.

Traceback II toimii kuten I-versiokin, mutta tiedoston pituus kasvaa vain 2930 tavulla. Viruksesta on myös kolmas, 3031 tavua pitkä versio.

Datacrime

Nimiä	Columbus
Tyyppi	tiedostovirus (COM)
Luokitus	erittäin vaarallinen

Datacrime-viruksesta on kaksi versiota, jotka molemmat tarttuvat COM-ohjelmiin. 1-versio kasvattaa tiedoston pituutta 1280:lla tavulla ja 2-versio 1168:lla tavulla. Virus jättää rauhaan kaikki sellaiset COM-tiedostot, joiden 7. kirjain on D. Näin se välttää myös tarttumasta COMMAND.COMiin. Tartunnan yhteydessä se etsii levyltä yhden puhtaan COM-tiedoston ja tarttuu siihen. Jos tiedoston minuuttien kolme alinta bittiä ovat samat kuin sekuntien kolme alinta bittiä, virus katsoo tarttuneensa jo tiedostoon ja jättää sen rauhaan.

Viruksen lempinimi "Columbus" aiheutuu sen tavasta aiheuttaa vahinkoa. Jos koneen päiväys on myöhäisempi kuin 12.10 (joka on Columbuksen päivä), se alustaa kiintolevyn 9 ensimmäistä uraa ja piippaa koneen kaiuttimesta. Urien tyhjentäminen riittää tuhoamaan kiintolevyn tiedostot. Samalla ruudulle tulostuu teksti

```
DATACRIME VIRUS
RELEASED: 1 MARCH 1989
```

Kakkosversio on parannettu malli edellisestä. Koodin parantaminen on myös lyhentänyt virusta hieman. Toiminnaltaan virus on täysin ykkösversion kaltainen.

Datacrime II on 1514 tavun mittainen virus, joka tarttuu sekä COM- että EXE-tiedostoihin. Versioita on ilmeisesti tehty hakuohjelmien harhauttamiseksi, sillä virukset on koodattu eri tavoin.

Viruksen tuhoaminen

Kone käynnistetään puhtaaksi tiedetyllä ja suojatulla DOS-levykkeellä. Saastuneet ohjelmatiedostot etsitään ja poistetaan levyltä.

Vienna

Nimiä	DOS-62, Unesco, Wieniläinen, 648, 1-in-8
Tyyppi	tiedostovirus (COM)
Luokitus	lievästi vaarallinen

Wieniläisvirus havaittiin ensi kertaa Moskovassa Unescon järjestämällä kesäleirillä. Virus tarttuu COM-tiedostoihin kasvattaen niiden pituutta 648 tavulla. Samalla virus muuttaa hakemistossa olevaa tiedoston kellonaikaa siten, että sekunneiksi tulee mahdoton arvo 62. Tämä ei näy käyttäjälle, sillä DOSin DIR-käsky näyttää ajasta vain tunnit ja minuutit.

Useimmista muista viruksista poiketen tämä virus ei missään vaiheessa jää keskusmuistiin. Kun viruksen saanut ohjelma käynnistetään, virus etsii levyltä puhtaan COM-tiedoston ja kopioi itsensä siihen. Uhria etsitään ensin oletushakemistosta ja kun kaikki sen COM-tiedostot on tartutettu, jatketaan tiedostojen hakua PATHin osoittamista hakemistoista. Kun kaikki PATH-hakemistotkin on käyty läpi, viruksen leviäminen loppuu. Uuden ohjelmatiedoston etsiminen ja viruksen kopiointi sen loppuun käy niin nopeasti, ettei käyttäjä usein-

kaan huomaa ylimääräistä viivettä ohjelman käynnistyksen yhteydessä. Ohjelmatiedostojen suojaaminen lukumääreellä tai niitä piilottamalla ei liioin estä virusta leviämästä.

Tartuntahetkellä virus tutkii koneen kelloa. Jos sekuntien määrä on kahdeksalla jaollinen, virus ei tartukaan uuteen ohjelmaan vaan kirjoittaa sen alun päälle viisi heksakoodia: EA F0 FF 00 F0. Ne muodostavat konekielisen hyppykäskyn JUMP F000:FFF0 joka saa koneen käynnistämään itsensä uudelleen (boot) kun ohjelmaa yritetään ajaa. Erittäin kiusallinen tilanne syntyy, jos tämä muutos osuu COMMAND.COMin kohdalle, koska tällöin konetta ei voi käynnistää muutoin kuin puhtaalta DOS-levykkeeltä. Kiintolevyltä käynnistäminen johtaa toistuvaan alkulatauskierteeseen, josta pääsee irti vain katkaisemalla koneesta sähköt ja käynnistämällä kone sen jälkeen alkuperäisellä DOS-levykkeellä.

Virusta pidetään lievästi vaarallisena, koska se tuhoaa noin joka kahdeksannen ohjelmatiedoston käyttökelvottomaksi. Tiedostoon tarttuneena se on kuitenkin vaaraton.

Virus on levinnyt varsin laajalle ja siitä on etsintäohjelmien hämäämiseksi tehty eri versioita (mm. Vienna-A ja Vienna-B). Eräs versio tavattiin marraskuussa 1989 Portugalissa, josta se sai nimen "portugalilainen". Tätä versiota on muutettu etsintäohjelmien hämäämiseksi niin, että jokaista ohjelmakäskyä on siirretty parilla tavulla eteenpäin. Lisäksi se kirjoittaa tiedoston alkuun "@AIDS" JMP-käskyn sijaan.

Viruksen tuhoaminen

Kone käynnistetään puhtaalla ja suojatulla DOS-levykkeellä. Saastuneet COM-tiedostot löytyvät yleensä PATHin osoittamista hakemistoista, mutta varmuuden vuoksi kannattaa tarkistaa muutkin hakemistot ja kaikki koneessa käytetyt levykkeet.

Ongelman muodostavat ne ohjelmat, jotka virus on tuhonnut kirjoittamalla hyppykäskyn tiedoston alkuun. Virusten etsintäohjelmat eivät yleensä anna näistä tiedostoista varoitusta, koska pilatun ohjelmatiedoston lopussa ei ole viruksen koodia. Varmuuden vuoksi kannattaakin käydä läpi kaikki COM-ohjelmat ja testata, toimivatko ne. Jos ohjelma

ei toimi vaan aiheuttaa alkulatauksen, on ohjelma syytä poistaa. Sitä ei voi edes puhdistaa, koska viisi ensimmäistä tavua on sotkettu.

Muita viruksia

Edellä lueteltujen merkittävien ja pitkään tunnettujen virusten lisäksi on liikkeellä suuri joukko viruksia, jotka ovat joko niin harvinaisia tai niin uusia, etteivät ne ole vielä ehtineet levitä laajalle. Kuten luettelo osoittaa, virusten tekijöiden kekseliäisyys tuntuu rajattomalta.

163. Pienin tunnettu PC-virus. Löydettiin kesäkuussa 1990 Islannista. Tarttuu kaikkiin COM-ohjelmiin kun ne käynnistetään, myös COMMAND.COMiin, ja kasvattaa niiden pituutta 163 tavulla, mutta ei tee varsinaista vahinkoa. Tartunnan saaneen tiedoston päiväys ja kellonaika muuttuu tartuntahetkeä vastaavaksi.

847. Virus on saanut nimensä määrästä, jolla se kasvattaa COM-tiedostojen pituuksia. Sisäisen laskurin edettyä tarpeeksi pitkälle se tulostaa ruudulle huvittavan ilmoituksen "Program sick error. Call doctor or buy PIXEL for cure description." mutta ei tee varsinaista vahinkoa. PIXEL viittaa lehteen, jossa viruksen listaus julkaistiin.

AIDS. Nimestään huolimatta tällä viruksella ei ole mitään tekemistä kirjan alussa mainitun AIDS-troijalaisen kanssa. Virus tarttuu COM- ja EXE-tiedostoihin , tulostaa ruudulle tekstin "Your computer now has AIDS" ja pysäyttää koneen.Virus kirjoittaa itsensä ohjelmatiedostojen alkuun tehden ne käyttökelvottomiksi.

AIDS II. Huhtikuussa 1990 löydetty virus, jonka toimintaperiaate on vähintäänkin omaperäinen. Virus ei tartu ohjelmatiedostoon lainkaan, vaan luo levylle saman nimisen COM-ohjelman, jonka pituus on 8064 tavua ja joka sisältää varsinaisen viruksen. Kun käyttäjä haluaa käynnistää esimerkiksi ohjelman nimeltä SOFTA.EXE, DOS käynnistääkin virusohjelman SOFTA.COM. Aina, kun virus luo levylle uuden ohjelmaa vastaavan COM-tiedoston, se soittaa koneen kaiuttimesta musiikkia sekä tulostaa ruudulle tekstin "Your computer is infected wth... Aids Virus II - signed WOP & PGT of DutchCrack-". Viruksen COM-tiedosto käynnistää alkuperäisen EXE-ohjelman ja kun se päättyy, ruudulle tulostuu vielä ilmoitus "Getting used to me? Next time, use a

Condom....." Koska virus ei tee mitään muutoksia alkuperäisiin EXE-tiedostoihin, on siitä helppo päästä eroon poistamalla kaikki EXE-tiedostoja vastaavat COM-virustiedostot.

Amoeba. Indonesiasta löydetty virus, joka tarttuu sekä COM- että EXE-tiedostoihin ja muuttaa niiden päiväyksen tartuntahetken mukaiseksi. Ei tee muuta vahinkoa. Viruksen nimi tulee sen sisältämästä tekstistä "SMA KHETAPUNK - Nouvel Band A.M.O.E.B.A".

Century. Jerusalem C-version variaatio, joka 1.1.2000 tuhoaa kaikki koneessa olevat levyt kirjoittamalla ne täyteen nollaa. Masentava alku uudelle vuosituhannelle, joka todellisuudessa alkaa vasta vuotta myöhemmin.

Den Zuk. Tarttuu 360-kilon levykkeiden käynnistyslohkoon. Eräät versiot sisältävät laskurin, jotka 5-10 asti päästyään alustavat asemassa olevan levykkeen, mutta useimmat viruksen versioista ovat vaarattomia. Tulostaa ruudulle punaisella "DEN ZUK" kun käyttäjä painaa CTRL-ALT-DEL. Pystyy poistamaan levykkeeltä muita viruksia ja istuttamaan itsensä niiden tilalle. Virus tarttuu vain 360 kilon lerpuille. Virus sisältää merkkijonon YC1ERP jonka uskotaan olevan viruksen tehneen indonesialaisen radioamatöörin kutsutunnus.

Devil's Dance. Löydettiin Mexico Cityssä joulukuussa 1989. Tarttuu samaankin COM-tiedostoon monta kertaa ja kasvattaa pituutta joka kerta 941 tavulla. Kun käyttäjä painaa CTRL-ALT-DEL, ruudulle tulostuu teksti "DID YOU EVER DANCE WITH THE DEVIL IN THE WEAK MOONLIGHT? PRAY FOR YOUR DISKS!! The Joker". 2000 näppäilyn jälkeen se alkaa muuntaa näytöllä olevan tekstin värejä ja 5000 näppäilyn jälkeen se sotkee FATin.

Fumble. COM-ohjelmiin tarttuva virus, joka aina silloin tällöin tuottaa kirjoitusvirheitä. Kun käyttäjä painaa esimerkiksi T-kirjainta, virus tulostaakin R-kirjaimen. Virus tarttuu vain kuukauden parittomina päivinä.

Ghost. Islantilainen virus, joka löydettiin lokakuussa 1989 Islannin yliopistosta. Sisältää tekstin "Ghostballs, Product of Iceland Copyright (c) 1989, 4418 and 5F19". Tarttuu COM-tiedostoihin kasvattaen niiden kokoa 2351 tavulla. Etsii levyltä ohjelmia, joihin tarttuu. Jos A: asemassa on 360 kilon levyke, virus kirjoittaa sille version Ping-Pong -viruksesta. Tämä versio ei ole varsinainen virus, koska se ei tartu,

mutta toimii myös 286- ja 386-koneissa. Ghost-virus on ainutlaatuinen sikäli, että se tarttuu *sekä* COM-ohjelmatiedostoihin *että* levykkeen käynnistyslohkoon.

Halloechen. Saksalainen virus, joka tarttuu sekä COM- että EXE-tiedostoihin kasvattaen niiden pituutta hieman yli 2 kilotavulla. Virus ei tartu tiedostoon, jonka kuukausi ja vuosi on sama kuin koneen kellossa. Aktivoituessaan virus sotkee näppäimistöltä annettavat merkit.

Itavir. Milanon teknillisessä korkeakoulussa maaliskuussa 1990 havaittu virus, joka tarttuu vain EXE-tiedostoihin kasvattaen niiden pituutta 3880 tavulla. Viruksen koodi sijaitsee tiedostossa, jonka nimen ensimmäinen merkki on näkymätön ja loppu "OMMAND.COM". Tämän tiedoston sisältö lisätään tartunnan saaneen ohjelman loppuun. Virus aktivoituu kun mikro on ollut päällä yli 24 tuntia yhtäjaksoisesti. Tällöin virus sotkee käynnistyslohkon ja tulostaa ruudulle italiankielisiä tekstejä.

Joker. Virus havaittiin ensimmäistä kertaa joulukuussa 1989 Puolassa. Virus tarttuu vain EXE-tiedostoihin ja joidenkin havaintojen mukaan se saattaa muuttaa myös DBF-tiedostojen sisältöä. Viruksen saastuttama ohjelma antaa huvittavilta kuulostavia virheilmoituksia: "I am hungry! Insert HAMBURGER into drive A:", "Water detect in Co-processor", "END OF WORKTIME. TURN SYSTEM OFF!" ja "In case mistake, call GHOST BUSTERS".

Kennedy. COM-tiedostoihin tarttuva virus, joka aktivoituu kolmena eri päivänä: 6.6. (Robert Kennedyn murhan päivä), 18.11. (Joseph Kennedyn kuolinpäivä) ja 22.11. (John F. Kennedyn murhan päivä) sotkien tällöin levyn tiedostoja. Viruksen sisältä löytyy teksti "The Dead Kennedys".

Korealainen. Käynnistyslohkovirus, joka on niin pieni, että koko virus mahtuu yhteen lohkoon. Alkuperäinen lohko siirretään Stoned-viruksen tapaan päähakemiston loppuun, lohkoon numero 11. Virus tarttuu myös kiintolevylle ja sotkee sen lohkoa siirtäessään. Nimensä virus on saanut Soulista, jossa se eristettiin ensi kertaa maaliskuussa 1990. Jo paria kuukautta myöhemmin se havaittiin Suomessa. Viruskoodin lopussa on arvoituksellinen teksti "virse program messge Njh to Lbc".

Lauantai 14 päivä. Tämä virus iskee lauantaina, joka osuu kuukauden 14 päiväksi tuhoten silloin A:, B: ja C: asemissa olevat levyt kirjoittamalla niiden varattujen aluiden päälle puppua. Virus on peräisin Etelä-Afrikasta ja sitä kutsutaan myös nimellä "Durban". Virus tarttuu sekä COM- että EXE-tiedostoihin ja kasvattaa niiden pituutta 669-684 tavulla. Ja juuri kun käyttäjä luuli selvinneensä perjantaista ja 13 päivästä...

Murphy. Eräs monista Dark Avengerin pohjalta tehdyistä viruksista, josta on useita versioita. Tarttuu sekä COM- että EXE-tiedostoihin kasvattaen niiden pituutta 1277 tavulla. Jos virus pääsee muistiin kello 10..11 se aiheuttaa epämääräistä ääntä koneen kaiuttimesta. Tasatunnein virus käynnistää koneen Basic-tulkin. Viruksen sisältä löytyy teksti "Hello, I'm Murphy. Nice to meet you friend. I'm written since Nov/Dec. Copywrite (c)1989 by Lubo & Ian, Sofia, USM Laboratory." Viruksen tekijä on nuori bulgarialainen mies.

Oropax. Tarttuu COM-tiedostoihin ja soittaa versiosta riippuen joko 3 (marssi, Straussin valssi ja Mozartin 41. sinfonia) tai 6 erilaista sävelmää 7 minuutin välein.

Pretoria. COM-tiedostoihin tarttuva virus, joka on peräisin Etelä-Afrikasta. Virus kasvattaa pituutta 879 tavulla. Virus ei jää keskusmuistiin vaan se etsii levyltä kaikki COM-tiedostot ja tartuttaa ne. Kesäkuun 16 päivä (Soweton mellakoiden vuosipäivä) virus tuhoaa päähakemiston ja FATit kirjoittamalla ne täyteen tekstiä "ZAPPED" ("pyyhitty").

Sunday. Ensimmäiset havainnot tästä viruksesta tehtiin Seattlessa, Washingtonissa marraskuussa 1989. Virus aktivoituu joka sunnuntai tulostaen ruudulle tekstin "Today is Sunday, why do you work so hard? All work and no play make you a dull boy! Come on! Let's go out and have some fun!". Virus on ilmeisesti tehty Jerusalemin pohjalle. Saattaa vahingoittaa FATia.

Sylvia. Virus sisältää tekstin "This program is infected by a HARMLESS Text-Virus V2.1, Send a FUNNY postcard to: Sylvia Verkade, Duinzoom 36b, 3235 CD Rockanje, The Netherlands. You might get an ANTIVIRUS program....." Ei tartu COMMAND.COMiin. Tekstissä mainittu tyttö on olemassa, mutta kieltää tuntevansa viruksen tekijää. Todennäköisesti kyseessä on joku hänen entisistä poikaystävistään.

Syslock. Tarttuu COM- ja EXE-tiedostoihin kasvattaen niiden kokoa 3551:llä tavulla. Luo levylle piilotetun tiedoston nimeltä IBMIONET.SYS, jossa lukee tieto siitä, miten pitkälle levyä kulloinkin on käsitelty. Virus käsittelee levyä 32 lohkon erissä ja muuntaa kaikki löytämänsä "Microsoft"-sanat "MACROSOFT"-sanoiksi. A-versio muuntaa sanat muotoon "MACHOSOFT". Virus ei tee mitään jos se löytää ympäristömuuttujan SYSLOCK ja sille annetun arvon @. Viruksen tekijä on ilmeisesti käyttänyt niksiä suojatakseen oman koneensa virukselta. Viruksesta on myös liikkeellä versio, joka soittaa joulukuussa "Oi kuusipuu".

Taiwan. Havaittiin ensi kertaa tammikuussa 1990 Taiwanissa. Tarttuu COM-tiedostoihin ja aktivoituu jokaisen kuukauden kahdeksantena päivänä tuhoten tällöin C: ja D: asemien kirjanpidot.

Ten bytes. Tarttuu sekä COM- että EXE-tiedostoihin, myös COMMAND.COMiin, ja kasvattaa tiedostojen pituutta 1554-1569 tavulla. Syys-joulukuun välisenä aikana se sotkee kaikki levylle kirjoitettavat tiedostot niin, että jokaisen tiedoston alusta puuttuu 10 tavua. Vastaava määrä satunnaisia tavuja lisätään tiedostojen loppuun, jotta tiedoston pituus ei näyttäisi muuttuvan. Tällaisen käsittelyn jälkeen kaikki ohjelmatiedostot ja useimmat työtiedostot ovat pilalla.

Toothless (V534). Neuvostoliitosta löydetty ja todennäköisesti siellä tehtykin virus, joka on rakennettu wieniläisen pohjalta. Virus tarttuu COM-tiedostoihin ja kasvattaa niiden pituutta 534 tavulla. Virus merkitsee tartuttamansa tiedostot muuttamalla kuukauden numeroksi 13. Kuukausinumero näkyy DIR-listauksesta, mikä tekee sen havaitsemisen helpoksi.

Vbasic. Toukokuussa 1990 löydetty virus, joka ei ole muistinvarainen, mutta tarttuu COM- ja EXE-tiedostoihin kasvattaen niiden pituutta 5120 tavulla. Saattaa sotkea tiedostoja. Viruksen iso koko johtuu siitä, että virus on tehty käännetyllä Basicillä.

XA1. Maaliskuussa 1990 Länsi-Saksasta löydetty virus, joka aktivoituus jouluisin (X) ja aprillipäivänä (A1). Virus tarttuu COM-tiedostoihin mutta ei ole muistinvarainen. Joulukuun 24-31 päivinä se tulostaa kuvaruudulle joulukuusen ja tekstin "Und er lebt doch noch: Der Tannenbaum! Frohe Weihnachen..." (Se elää sittenkin: joulukuusi!

Hauskaa joulua...). Aprillipäivänä virus tuhoaa nollauran kirjoittamalla sen täyteen tekstiä "April".

Uusia, entisiä tehokkaampia ja vaarallisempia viruksia on tarkasteltu kahdeksannessa luvussa.

7

Virusten torjuntaohjelmat

Koska virukset ovat ohjelmia, niitä voidaan etsiä ja torjua toisilla ohjelmilla. Virusten määrän lisääntyminen on herättänyt ohjelmoijat ja tarjolla on nykyisin lukuisia erilaisia torjunta-, parannus- ja suojautumisohjelmia. Koska ohjelmien hinnassa, toimintaperiaatteessa ja tehokkuudessa on suuria eroja, kannattaa harkita tarkkaan mitä ohjelmia käyttää. Seuraavassa on esitelty erilaisia torjuntaohjelmia ja kerrottu niiden hyvistä ja huonoista puolista.

Ohjelmien luokittelu

Virusten ja troijalaisten torjuntaan tarkoitetut ohjelmat voidaan jakaa seitsemään ryhmään niiden toimintaperiaatteen mukaisesti:

1. Yleiset apuohjelmat (Norton, PC-Tools, CHKDSK yms.), joita voidaan muiden toimintojen ohella käyttää virusten etsintään ja havaitsemiseen.

2. Virusten etsintäohjelmat (McAfee Scan, IBM Virscan yms.), jotka etsivät levyllä piileskeleviä viruksia niiden "sormenjälkien" avulla.

3. Tarkistussumman käyttöön perustuvat ohjelmat, jotka antavat varoituksen mikäli ohjelmatiedoston pituus tai sisältö muuttuu.

4. Muistinvaraiset torjuntaohjelmat, jotka pyrkivät estämään virusten ja troijalaisten vahingonteon esimerkiksi kieltämällä kaikki suorat kirjoitusyritykset levylle.

5. Tutkimisohjelmat, joilla saatu ohjelma voidaan analysoida virusten ja troijalaisten havaitsemiseksi ennen sen ajamista.

6. Tietoturvaohjelmat, jotka pyrkivät estämään mikron asiatonta käyttöä ja sallivat vain ennalta tutkittujen ja hyväksyttyjen ohjelmien käynnistämisen.

7. Muut ohjelmat. Tähän ryhmään kuuluvat mm. levykkeiden ja tiedostojen "rokottamiseen" tarkoitetut ohjelmat sekä virusten poisto-ohjelmat.

Jokaisella ohjelmatyypillä on omat hyvät ja huonot puolensa eikä mikään ohjelma ei yksistään riitä antamaan täydellistä suojaa viruksia vastaan. Paras suoja saadaan käyttämällä useita ohjelmia yhtä aikaa.

Kaupallinen vai ilmainen?

Virusten torjuntaan on saatavissa sekä kaupallisia että ei-kaupallisia tuotteita. Ohjelman hinta ei välttämättä takaa sen laatua - monet parhaista ohjelmista ovat joko täysin ilmaisia PD-ohjelmia tai sitten niiden tekijä toivoo saavansa pienen korvauksen jos käyttäjä toteaa ohjelman itselleen hyödylliseksi (shareware). Ohjelmilla on usein kuvaavia nimiä: aspirin, datacure, condom, flushot.

Ei niin hyvää ettei jotain pahaakin. Tiedetään tapauksia, joissa ilmainen torjuntaohjelma on itse asiassa levittänyt virusta tai ollut vahinkoa tuottava Troijan hevonen. Tässäkin asiassa kannattaa noudattaa varovaisuutta ja käyttää vain sellaisia ohjelmia, joista muilla on jo kokemuksia.

Seuraavaksi tarkastellaan lähemmin eri ryhmiin kuuluvia torjuntaohjelmia. Kunkin ohjelmaryhmän kohdalla esitellään sen toimintape-

riaate, hyvät ja huonot puolet sekä esitellään muutamia ryhmän ohjelmista yksityiskohtaisemmin.

Ohjelmien luokittelu toimintaperiaatteen mukaan alkaa olla vaikeata, sillä kun ohjelmia on kehitetty, on niihin lisätty eri periaatteilla toimivia osia. On myös kokonaisia torjuntapaketteja, joista löytyy ohjelma jokaista eri ryhmää varten.

1. Yleiset apuohjelmat

PC-Tools ja Norton Utilities ovat kilpailleet tasaväkisesti käyttäjien suosiosta jo monen vuoden ajan. Suomessa PC-Tools on ollut suositumpi paremman mainonnan ja suomeksi käännetyn opaskirjan ansiosta. Ohjelman uusimmat versiot sisältävät suuren joukon pieniä työkaluja aina tietoliikennettä, tekstinkäsittelyä, laskukonetta, muistikirjaa ja pientä tietokantaa myöten. Ainoa, mitä PC-Tools ei vieläkään osaa, on kahvin keittäminen.

Norton Utilities -paketissa on kokonaan toisenlainen toiminta-ajatus. Se ei yritäkään tehdä kaikkea, vaan tarjoaa pelkkiä levynkäytön apuohjelmia. PC-Toolsista poiketen ohjelmat ovat erillisiä ja kooltaan pieniä, jolloin käyttäjä voi kopioida niistä levylle vain tarvitsemansa. Ohjelmat eivät ole PC-Toolsin tapaan valikko-ohjattuja, vaan niitä käytetään DOSin omien apuohjelmien tapaan komentoriviltä annettavilla parametreilla. Varmuuskopiointia, tiedostojen muokkausta ja helppokäyttöistä DOS Shelliä varten Nortonilta löytyvät omat ohjelmansa (Norton Backup, Norton Editor ja Norton Commander). Ohjelmista Norton Commander on saatavissa myös suomennettuna versiona.

Kolmas, Suomessa ja maailmalla paljon vähemmälle huomiolle jäänyt yleiskäyttöinen apuohjelmapaketti on Mace Utilities. Eräs paketin mukana tulevista ohjelmista on suoraan virustorjuntaan tarkoitettu Vaccine. Muutoin Macesta löytyvät suunnilleen Nortonin kaltaiset toiminnot.

Kaikissa edellä luetelluissa ohjelmissa on osuus, jolla voidaan lukea ja kirjoittaa levyä mistä kohtaa tahansa. Esimerkiksi Nortonilla käyttäjä voi kurkistaa suoraan päähakemistoon, levyn käynnistyslohkoon tai kiintolevyn nollauralle ja jopa muuttaa niissä olevia tietoja. Muutosten

Root dir — Directory format
Sector 130 in root directory — Offset 480, hex 1E0

Filename	Ext	Size	Date	Time	Cluster	Arc	R/O	Sys	Hid	Dir	Vol
386SPART	PAR	2091008	26.06.90	16.25	5973	Arc		Sys	Hid		
COMMAND	COM	28669	31.08.89	12.00	80	Arc					
CONFIG	SYS	224	29.05.90	22.17	5974	Arc					
SD	INI	2497	24.03.90	10.14	5975	Arc					
BASEDD01	SYS	57413	31.08.89	12.00	5977	Arc					
OS2LDR		14336	31.08.89	12.00	5504	Arc			Hid		
OS2KRNL		339770	31.08.89	12.00	5511	Arc			Hid		
EA DATA	SF	327680	16.03.90	23.57	11555	Arc	R/O	Sys	Hid		
FRECOVER	IDX	29	26.06.90	16.47	16319	Arc	R/O	Sys	Hid		
FRECOVER	DAT	50688	26.06.90	16.47	6006	Arc	R/O				
FRECOVER	BAK	50688	26.06.90	16.47	6031	Arc	R/O				
CONFIG	OLD	122	13.02.90	20.10	6056	Arc					
HIMEM	SYS	11304	1.05.90	3.00	6057	Arc					
SU2301		441195	24.06.90	22.54	14738	Arc					
HELP	CRC	12070	7.04.90	11.22	6064	Arc					
STARTUP	CMD	410	11.05.90	21.13	6070	Arc					

Filenames beginning with 'σ' indicate erased entries
Press Enter to continue

1Help 2Hex 3Text 4Dir 5FAT 6Partn 7 8Choose 9Undo 10QuitNU

Kun Nortonilla katsotaan suoraan levyä, nähdään myös piilotettujen tiedostojen nimet ja pituudet. Kuvassa kiintolevyn päähakemisto Nortonin näkemänä. 386SPART.PAR on Windows 3:n luoma pysyvä virtuaalimuistialue. OS2LDR ja OS2KRNL ovat OS/2:n piilotettuja käyttöjärjestelmätiedostoja. DOSin vastaavat tiedostot sijaitsevat heti levyn alussa eivätkä näy esimerkin kuvassa. FRECOVER-tiedostot ovat Nortonin FR-ohjelman luomia varmuuskopioita FATeista ym. varatuista alueista.

tekemisessä on parasta olla erittäin varovainen, sillä varatuille alueille kirjoittaminen saattaa tehdä levystä käyttökelvottoman. Jos CHKDSK kertoo levyllä olevan tavallista enemmän piilotettuja tiedostoja, on niiden nimet ja pituudet helpointa selvittää kurkistamalla ohjelman avulla suoraan hakemistoon.

Nortonin tutkimisosa on PC-Toolsin vastaavaa kehittyneempi. Se on myös mukavampi käyttää, koska Norton näyttää levyltä 512 tavua kerrallaan kun näytön koko PC-Toolsissa on vain 256 tavua. Osa tämän kirjan kuvista on otettu Nortonin näytöstä.

Norton Utilities tuli aikoinaan tunnetuksi siitä, että se oli ensimmäinen ohjelma joka mahdollisti vahingossa poistettujen tiedostojen palauttamisen takaisin käyttöön. Ohjelmasta tuli monelle käyttäjälle pakollinen pelastusrengas, jota ilman mikron käyttö tuntui pelottavalta.

Sittemmin palautusmahdollisuus on lisätty myös moniin muihin apuohjelmiin, mm. PC-Toolsiin. Ominaisuudesta on hyötyä, mikäli virus ehtii poistaa tärkeitä tiedostoja. Ohjelmien avulla voi myös kurkistaa bad sectoriksi merkittyyn alueeseen ja tarkistaa, mitä se pitää sisällään.

Jos virus pääsee tuhoamaan levyn, on jonkin levytyökalun käyttö ainoa tapa pelastaa edes osa tiedostoista. FATin parsiminen takaisin kasaan Nortonin, Macen tai PC-Toolsin avulla on periaatteessa mahdollista, mutta käytännössä erittäin työlästä.

Mikäli ohjelmia käytetään koneessa, jossa virus on iskenyt tai jossa edes epäillään olevan viruksia, on ohjelmat muistettava käynnistää kirjoitussuojatulta levykkeeltä.

PC-Toolsiin kuuluu osuus, joka näyttää keskusmuistissa olevat ohjelmat. Tällaisia ohjelmia on saatavissa myös erikseen PD:nä. Virustorjunnassa ohjelmista ei ole suurtakaan apua, sillä muistikartan tutkiminen edellyttää melkoista asiantuntemusta. Lisäksi monet virukset osaavat piilottaa itsensä niin hyvin, etteivät ne välttämättä näy listalla.

2. Etsintäohjelmat

Käyttäjän kannalta helpoimpia ovat ohjelmat, jotka etsivät viruksia suoraan levyltä. Ohjelman muistissa on tunnettujen virusten "sormenjälkiä" (signature) eli pieniä pätkiä niiden ohjelmakoodista. Jos näitä merkkejä havaitaan levyllä olevista tiedostoista, annetaan virusvaroitus.

Etsintäohjelmaa tehtäessä törmätään mielenkiintoiseen ongelmaan. Jotta ohjelma voisi tunnistaa viruksen, sen on pidettävä muistissaan eri virusten sormenjälkiä. Jäljet saattavat olla myös erillisessä tiedostossa levyllä, josta ne luetaan muistiin etsinnän alkaessa. Miten estää toista etsintäohjelmaa luulemasta näitä sormenjälkiä oikeiksi viruksiksi?

Väärien hälyytysten välttämiseksi on etsintäohjelmien käyttämät sormenjäljet koodattu. Koodaus onkin helppo tehdä. Jo se, että jokaisesta bittiarvosta vähennetään tietty vakioarvo (vaikka yksi), riittää. Ykkönen lisätään takaisin vasta vertailuhetkellä. Toinen mahdollisuus on käyttää virusten ohjelmakoodin sijasta koodin heksadesimaalisia

vastineita, jotka vasta keskusmuistissa muutetaan binääriarvoiksi. Tämäkin saattaa tuottaa vääriä hälyytyksiä, jos virusohjelma tarkistaa keskusmuistin ja löytää sieltä edellisen etsintäohjelman käyttämiä sormenjälkiä.

Etsintäohjelmat ovat helppoja käyttää ja toimivat kohtuullisen nopeasti. Isonkin kiintolevyn ohjelmatiedostot on yleensä käyty läpi muutamassa minuutissa. Etsintä kestää kuitenkin sen verran pitkään, ettei sitä kannata lisätä AUTOEXEC.BATiin. Jos viruksia havaitaan, ohjelma kertoo mikä virus on kyseessä sekä saastuneiden ohjelmien nimet. Muutamat etsintäohjelmat pystyvät poistamaan saastuneet tiedostot tai parantamaan tiedoston niin, että siinä oleva virus tuhotaan.

Etsintäohjelmia käytettäessä kannattaa muistaa yksinkertainen sääntö: jos ohjelma löytää viruksen, se on yleensä olemassa, mutta ellei virusta löydy, se ei välttämättä tarkoita etteikö sitä olisi. Etsintäohjelma voi tunnistaa vain sellaiset virukset, jotka sen tekijäkin on tuntenut. Koska uusia viruksia syntyy koko ajan, ei mikään ohjelma voi tuntea niitä kaikkia. Samasta syystä etsintäohjelmia on päivitettävä jatkuvasti, jotta ne pysyisivät tunnettujen virusten tasalla.

Muistiin päästyään voivat eräät virukset huijata etsintäohjelmia niin, etteivät nämä löydä viruksia, jotka ne muutoin tuntisivat. Näin menettelee mm. Brain-virus, joka piileskelee käynnistyslohkossa ja antaa etsintäohjelmalle sen pyytäessä alkuperäisen, virheettömän käynnistyslohkon.

Jos epäillään, että mikrossa on virus, pitäisi kone käynnistää puhtaalta DOS-levykkeeltä ja hakuohjelma ajaa kirjoitussuojatulta levykkeeltä. Näin voidaan varmistaa se, ettei muistissa oleva virus pysty hämäämään etsintäohjelmaa eikä tarttumaan siihen.

Joskus harvoin virusten etsintäohjelmat voivat aiheuttaa myös vääriä hälyytyksiä. Jos etsinnässä käytetyt sormenjäljet ovat epämääräisiä tai liian lyhyitä, saattavat ne täsmätä aivan viattomienkin tiedostojen kanssa. Esimerkiksi McAfeen Scan-ohjelman versio 2.0V56 antaa /A-valitsinta käytettäessä hälyytyksen 4096-viruksesta Flight Simulator 4.0-version tiedostossa MONO.GRA, vaikka tiedosto onkin täysin puhdas. Uudemmissa Scan-versioissa tämä virhe on korjattu, mutta muita vääriä hälyytyksiä saattaa silti sattua vieläkin.

Seuraavassa on esitelty joukko etsintäohjelmia. Vanha ja hyväksi havaittu McAfeen Scan on saanut koko joukon kilpailijoita sen jälkeen kun ohjelmoijat ovat huomanneet viruspelosta syntyneet kaupalliset mahdollisuudet.

IBM Virscan

IBM:n tulemista uudelle alueelle pidetään usein merkkinä siitä, että ala on saavuttanut "virallisen hyväksynnän". Tällä kriteerillä mitaten PC-viruksista tuli virallisesti tunnustettu uhka syksyllä 1989 kun IBM julkisti oman virusten etsimisohjelmansa, VIRSCANin. Ohjelma on kaupallinen, mutta IBM myy sitä omakustannushintaan parilla sadalla markalla.

IBM:n Virscan on tärkeä ohjelma siksi, että kun yritys alkaa etsiä virusten torjuntaohjelmaa, on IBM:n ohjelma helpoin hankkia. Se löytyy useimmilta IBM:n jälleenmyyjiltä - ja heitä on paljon - samasta hinnastosta kuin muutkin sovellusohjelmat ja tietokonelaitteet. Julkisohjelmien hankinta on paljon vaikeampaa - ainakin, jos ei satu tuntemaan mikroharrastajia.

IBM:n etsintäohjelma on nimeltään VIRSCAN.EXE. Sen tuntemat virukset luetellaan kahdessa tekstitiedostossa: SIGBOOT.LST (levykevirukset) ja SIGFILE.LST (tiedostovirukset). Tiedot luetaan muistiin ennen etsinnän aloittamista. Tiedostossa on lueteltu kunkin viruksen nimi sekä etsintään käytetty "sormenjälki" heksadesimaalimuodossa. Koska koodit eivät ole binäärimuodossa, eivät ne häiritse toisia etsintäohjelmia. Itse etsintäohjelma on perhesovellus, joten sitä voi ajaa myös OS/2:n merkkipohjaisessa tilassa.

Virscanin ensimmäiset versiot eivät tunteneet kovinkaan monta virusta. Ohjelma saattoi jopa levittää muistissa olevaa Dark Avengeria huomaamatta itse asiaa lainkaan. Uudemmissa versioissa ohjelmaa on parannettu niin, että se tarkistaa aluksi keskusmuistin ja aloittaa tiedostojen tutkimisen vasta jos keskusmuisti havaitaan puhtaaksi. Tunnettujen virusten määrää on lisätty LST-tiedostoja päivittämällä.

```
C:\>VIRSCAN C:

(C) Copyright IBM Corporation 1989, 1990
Virus scanner      Version 1.41
Starting virus scan on Sat Apr 07 22:51:45 1990
Scanning system memory for dangerous and/or well hidden resident
viruses
Found signature in (C:\PROG\TARKIN.EXE) at offset 12650 (316AH)
8ED0BC000750B8C50050CBFC062E8C0631002E8C0639002E8C063D002E8C0641
008CC0
This file may be infected with the 1813(Jerusalem) virus.
(Continuing Scan)

Found signature in (C:\PROG\TARKIN.EXE) at offset 14458 (387AH)
8ED0BC000750B8C50050CBFC062E8C0631002E8C0639002E8C063D002E8C0641
008CC0
This file may be infected with the 1813(Jerusalem) virus.
(Continuing Scan)

Found signature in (C:\PROG\TARKIN.EXE) at offset 16266 (3F8AH)
8ED0BC000750B8C50050CBFC062E8C0631002E8C0639002E8C063D002E8C0641
008CC0
This file may be infected with the 1813(Jerusalem) virus.
(Continuing Scan)

Scan completed.
82 files were scanned.
1 system boot sector was scanned.
1 master boot record was scanned.
Total bytes scanned = 3427392, in 62 seconds.
3 Viral signatures found.
```

IBM:n VIRSCAN on havainnut Jerusalem B:n tarttuneen kolme kertaa TARKIN.EXE-tiedostoon.

McAfee Viruscan

McAfeen ohjelmista on tunnetuin Viruscan, jota yleensä kutsutaan lyhyemmin nimellä Scan. Tämä on myös ajokelpoisen ohjelman nimi. Ohjelma on sharewarea ja tekijä odottaa saavansa siitä 25 dollarin korvauksen. Tämän McAfee on ansainnutkin, sillä Scan on helppokäyttöinen ja luotettava. Lisäksi siitä ilmestyy säännöllisesti uusia, ajanmukaistettuja versioita.

Koska Scania levitetään lähinnä purkkien välityksellä, on tekijä pyrkinyt takaamaan ohjelmansa luotettavuuden eri tavoin. Mukana tulee mm. tiedosto, josta käy ilmi alkuperäisestä SCAN.EXE-

tiedostosta laskettu tarkistussumma sekä VALIDATE-niminen ohjelma tämän summan laskemiseksi. Näillä käyttäjä voi varmistaa, ettei kukaan ole matkan varrella tehnyt ohjelmaan omia lisäyksiä tai istuttanut siihen virusta. Sormenjäljet, joita virusten etsinnässä käytetään, on koodattu ja upotettu ohjelman sisään, jotta kukaan ei pysty muuttamaan niitä.

Virusten etsiminen voidaan rajoittaa yhteen tiedostoon, yhteen hakemistoon tai kohdistaa koko levyyn. A: asemassa olevan levykkeen tarkistaminen käy kirjoittamalla

```
C:\SCAN>SCAN A:
```

Jos halutaan tarkistaa vain yksi hakemisto ja sen tiedostot, kirjoitetaan hakemiston nimi heti ohjelman nimen perään. Komento

```
C:\SCAN>SCAN C:\PD
```

tarkistaa \PD-hakemistossa olevat tiedostot. Yksi nimeltä mainittu tiedosto tarkistetaan kirjoittamalla tiedoston nimi esimerkissä olevan hakemiston paikalle.

Aina, kun Scan käynnistetään, se tarkistaa ensin itsensä. Jos ohjelmaan itseensä on tarttunut virus tai joku on muutoin peukaloinut SCANia, tulostuu virheilmoitus "Warning, file has been damaged" eikä virusten etsimistä aloiteta. Tarkistus ei tosin näytä toimivan luotettavasti eräiden uusien tehovirusten kohdalla.

Seuraavaksi Scan tarkistaa nopeasti keskusmuistin. Tarkistus tehdään sellaisten virusten varalta (mm. Dark Avenger), jotka leviävät jo tiedoston avauksen yhteydessä.

Jos muistista löytyy aktiivinen Dark Avenger-virus, ohjelma pysähtyy ja tulostaa varoituksen:

```
SCAN 3.5V63 Copyright 1989-90 by McAfee Associates.
(408) 988-3832
Scanning for known viruses.
Scanning 64K RAM
  Found Dark Avenger virus [Dav] active in memory.
Scanning 640K RAM
```

McAfeen virustentorjuntaohjelmat

John McAfee on amerikkalainen virusten etsintään ja torjuntaan erikoistunut asiantuntija. Hänen yrityksensä (McAfee Associates, 4423 Cheeney Street, Santa Clara, CA 95054, puh 408 988 3832, BBS-yhteys 408 988 4004, Suomesta soitettaessa eteen tulevat numerot 990-1) valmistaa useita virusten etsintään ja tuhoamiseen tarkoitettuja ohjelmia.

McAfeen ohjelmat ovat ns. shareware-tuotteita. Niitä saa kokeilla ja testata vapaasti, mutta ohjelmien säännöllinen käyttö edellyttää rekisteröintiä. Tämä tapahtuu lähettämällä rekisteröintikaavake sekä ohjelmista pyydetty korvaus tekijälle. Rekisteröitynyt käyttäjä saa myös tarvitessaan teknistä apua viruksen poistamiseen McAfeen BBS-numerosta. Maksaminen käy helpoiten ilmoittamalla Visa-kortin numero rekisteröinnin yhteydessä. Yhdeksän dollarin lisähinnalla McAfee lähettää paluupostissa rekisteröityjen ohjelmien uusimmat versiot 360 kilon levykkeellä. Levyke tulee noin parin viikon kuluttua rekisteröinti-ilmoituksen lähettämisestä.

McAfeen shareware-ohjelmia ovat:

- ☐ VIRUSCAN (SCAN.EXE). Virusten etsimisohjelma. Rekisteröintimaksu $25.
- ☐ NETSCAN (NETSCAN.EXE). Virusten etsintäohjelma lähiverkkoa varten. Palveluaseman levyn voi tarkistaa työasemasta käsin. Rekisteröinti $25.
- ☐ CLEAN-UP (CLEAN.EXE). Viruksen saastuttamien tiedostojen ja levykkeiden puhdistusohjelma. Rekisteröintimaksu $35.
- ☐ VSHIELD (VSHIELD.EXE, aiemmin nimellä SCANRES). Muistinvarainen ohjelma, joka tarkistaa jokaisen käynnistettävän ohjelman ennen kuin se päästetään muistiin.
- ☐ SENTRY (SENTRY.EXE). Nopea tarkistussummien laskentaan perustuva ohjelma.
- ☐ VCOPY (VCOPY.EXE). COPY-käskyn korvike, joka tarkistaa tiedostot virusten varalta kopioidessaan niitä.

```
Power down the system immediately.
Reboot from a clean, write protected system
diskette and re-run SCAN to determine extent of
hard disk infection.
```

Tarkistus kehottaa sammuttamaan koneen välittömästi ja käynnistämään sen uudelleen puhtaaksi tiedetyllä DOS-levykkeellä. Vasta tämän jälkeen tulee SCAN-ohjelma ajaa uudelleen, jotta tartunnan laajuus saadaan selvitettyä ja tiedostot puhdistettua.

Ellei pikaista muistitarkistusta olisi, Scan levittäisi muistissa aktiivisena olevan viruksen kaikkiin tutkimiinsa ohjelmatiedostoihin. Muistitarkistus voidaan ohittaa valitsimella /nomem. Perusteellinen muistitarkistus saadaan käyttämällä /M-valitsinta. Tällöin Scan tarkistaa keskusmuistin kaikkien tuntemiensa virusten varalta. Ellei konetta ja etsintäohjelmaa ole käynnistetty puhtaalta DOS-levykkeeltä, kannattaa muistitarkistus aina tehdä. Se on mm. ainoa tapa havaita muistissa aktiivisena oleva Brain-virus, joka osaa huijata etsintäohjelman käyttämiä levykäskyjä.

Scan tarkistaa levyn käynnistyslohkon, mahdolliset käyttöjärjestelmätiedostot sekä kaikki EXE-, COM-, SYS-, PIF-, OVR-, OVL-, OVG-, OV1- ja OV2-tiedostot. Kiintolevyllä tarkistetaan myös osiotaulukko. /A -valitsimella käynnistettynä ohjelma käy läpi kaikki levyn tiedostot, mikä kestää monta kertaa kauemmin kuin pelkkien ohjelmatiedostojen tarkistaminen.Virusten lisäksi Scan etsii myös AIDS ja Twelve Tricks Troijalaisia.

Jos viruksia löytyy, Scan ilmoittaa saastuneen tiedoston nimen sekä viruksen nimikoodin. Kun tämä koodi ja tiedoston nimi annetaan Clean-puhdistusohjelmalle, saadaan tiedosto puhdistettua. /D-valitsinta käytettäessä Scan pysähtyy jokaisen saastuneen tiedoston kohdalla ja kysyy, poistetaanko se. Jos vastaus on myönteinen, Scan käy ensin kirjoittamassa tiedoston päälle nollaa ja lopuksi poistaa sen. Mikäli virus löytyy käynnistyslohkosta, osiotaulukosta tai joltain muulta varatulta alueelta, on poistaminen tehtävä Clean-puhdistusohjelmalla.

Komento

```
C:\SCAN>SCAN C:\OMAT /D /M
```

```
C:\SCAN>SCAN A:
SCAN 3.5V63 Copyright 1989-90 by McAfee Associates.
(408) 988-3832
Scanning for known viruses.
Scanning 640K RAM
Scanning boot sector of disk A:
  Found Ping Pong Virus - Version B [Ping] in boot
sector.
Scanning A:\LOAD.COM
  Found Jerusalem Virus Strain B [Jeru]
Scanning A:\FL.EXE
  Found Dark Avenger virus [Dav]
Scanning A:\MOUSE.COM
  Found 1701/1704 Virus - Version B [170X]
Scanning A:\COMP.COM
  Found Yankee Doodle Virus [Doodle]

 Found 4 files containing viruses.
```

Mikrotukihenkilön painajainen: McAfeen etsintäohjelma on löytänyt levyltä neljä eri virusten saastuttamaa tiedostoa. Lisäksi levykkeen käynnistyslohkosta on löytynyt Ping Pong-virus.

suorittaa täyden muistitarkistuksen, etsii saastuneita tiedostoja C:\OMAT-hakemistosta ja poistaa ne.

Lähiverkkoja varten Scan-ohjelmasta on olemassa oma Netscan-versio. Se tarkistaa vain verkossa olevat tiedostot, eikä yritäkään lukea palveluaseman käynnistyslohkoa tai nollauraa, koska se ei onnistuisi verkon läpi.

Scan-ohjelmasta on olemassa myös muistinvarainen versio VShield. Kun tämä ohjelma ladataan keskusmuistiin, se tarkistaa jokaisen käynnistettävän ohjelman ennen sen ajoa. Vshield kuluttaa noin 20 kilotavua keskusmuistia. Tarkistus tapahtuu niin nopeasti, ettei se hidasta havaittavasti ohjelman käynnistämistä.

McAfee valmistaa myös kaupallista etsintä- ja puhdistusohjelmaa nimellä PROSCAN. Siinä on valikko-ohjattu käyttöliittymä.

F-PROT-virussuojaa Islannista

Virusten torjuntaohjelmia tehdään myös täällä pohjolassa. Tunnetuin on islantilaisen Fridrik Skulasonin F-PROT -niminen paketti, johon kuuluu useita erilaisia apuohjelmia. Koska F-PROT on pohjoismainen tuote, ei se ole levinnyt maailmalla yhtä laajalle kuin vastaavat amerikkalaiset ohjelmat. Islannissa F-PROTia myydään kaupallisena tuotteena. Islannin ulkopuolella FPROTia saa jakaa vapaasti. Ohjelman käyttäjäksi rekisteröityminen maksaa kuitenkin $15 ja se oikeuttaa ilmaisiin ohjelmapäivityksiin.

Tärkeimmät F-PROT 1.10-version ohjelmista ovat:

F-DRIVER: laiteohjain, joka CONFIG.SYSiin asennettuna estää viruksen saastuttamien ohjelmien ajamisen
F-OSCHK: tarkistaa käyttöjärjestelmätiedostot virusten varalta
F-LOCK: muistinvarainen vartijaohjelma
F-SYSCHK: tarkistaa keskusmuistin virusten varalta
F-FCHK: etsii tiedostoviruksia levyltä ja poistaa ne haluttaessa
F-DISINF: etsii levykeviruksia ja poistaa ne haluttaessa
F-XLOCK: lisää ohjelmiin automaattisen virustarkistuksen
F-UNLOCK: poistaa edellisen
F-XCHK: sallii vain F-XLOCKilla muokattujen ohjelmien ajon
F-RUN: ajaa ohjelmia F-XCHK:n ollessa käytössä
F-INOC: "rokottaa" levykkeitä Brain- ja Ping Pong-viruksia vastaan
F-DLOCK: estää kiintolevyn alustamisen ja sille kirjoittamisen
F-DIR: tulostaa piilotettujen ja suojattujen tiedostojen nimet
F-MMAP: näyttää keskusmuistissa majailevat ohjelmat
F-BOOT: näyttää käynnistyslohkon sisällön
F-PBR: näyttää osiotaulukon (MBR) sisällön

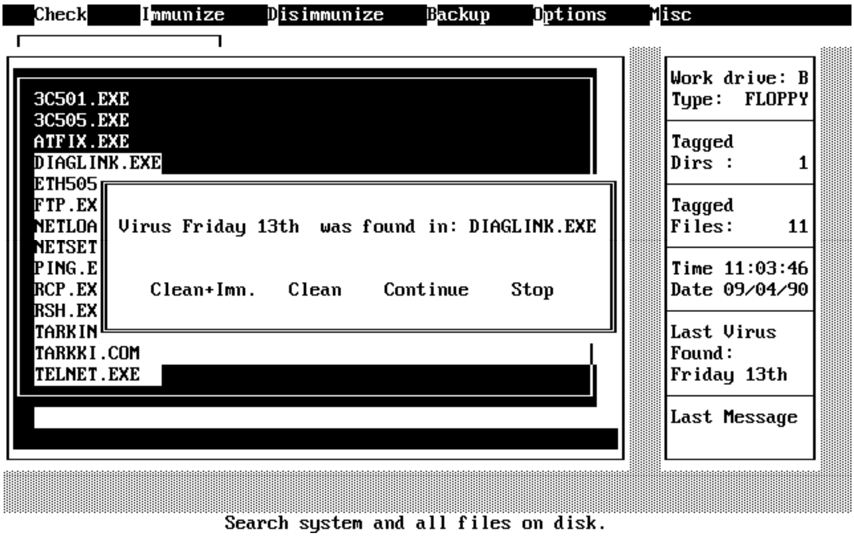
Eräitä pakettiin kuuluvia ohjelmia on käsitelty tarkemmin tekstissä eri ryhmien kohdalla.

F-PROTia koskevia parannusehdotuksia ja kommentteja voi lähettää tekijälle osoitteeseen Fridrik Skulason, Box 7180, IS-127 Reykjavik, Iceland.

Turbo Anti-Virus

Lähes kaikki viruksia vastaan kehitetyt ohjelmat näyttävät perin aneemisilta. Niiden käyttöliittymästä näkee, että ohjelmat on kehitetty asiantuntijoita, ei loppukäyttäjiä varten. Jo lennokkaan nimensä puolesta erottuva Turbo Anti-Virus -ohjelmisto on toista maata. Ikkunoita, värejä, valikoita ja ääniefektejä käyttämällä ohjelmasta on saatu näyttävä ja suorastaan ilo käyttää. Vaihtoehtoisesti ohjelmaa voi käyttää myös komentoriviltä annettavilla parametreilla.

Turbo Anti-Viruksen takana on israelilainen Carmel Software Engineering. Tekijöiden joukossa on paikallisessa virusjahdissa kunnostautuneita henkilöitä. Pakettiin kuuluu kaksi ohjelmaa, joista TNTVIRUS on tarkoitettu virusten etsimiseen ja poistamiseen. Poistamisen yhteydessä ohjelma palauttaa viruksen varaamat bad sector-alueet takaisin käyttöön. Ohjelmalla voi lisäksi rokottaa levykkeitä ja tehdä varmuuskopioita käyttöjärjestelmän varatuista alueista ja laskea niistä tarkistussummia.



Israelilainen TNT Antivirus eroaa muista torjuntaohjelmista näyttävän käyttöliittymänsä vuoksi.

Turbo Anti-Viruksella on vuoden takuu, jonka aikana ohjelmasta toimitetaan ilmaiset päivitykset, mikäli uusia viruksia löytyy. Ohjelma on hämmästyttävää kyllä kopiosuojattu. Verkkoversio on saatavissa erikseen.

Turbo Anti-Virus ja eräät muut vastaavat ohjelmat mainostavat itseään sillä, että ne hoitavat yhdellä ohjelmalla kaikki virusten torjunnan ja suojautumisen osa-alueet. Samat toiminnot voisi koota myös ilmaisista tai edullisista shareware-ohjelmista, mutta tällöin käyttäjälle jää kokoamisen, asentamisen ja suunnittelun vaiva. Voisi myös olettaa, että kaupallisten ohjelmien tuotetuki toimisi paremmin, mutta tämä ei läheskään aina pidä paikkaansa.

HCOPY ja VCOPY

Vuoden 1990 kevät-Comdex pidettiin 3-6 kesäkuuta Atlantassa. Hilgrave, joka tunnetaan HyperAccess-nimisestä tietoliikenneohjelmastaan, julkisti messujen aikana HCOPY-nimisen apuohjelman ja lahjoitti sen vapaaseen jakeluun. Ohjelmallaan Hilgrave halusi samalla mainostaa tietoliikenneohjelmaansa, johon on lisätty sisäänrakennettu virustarkitus.

HCOPY-ohjelman toimintaperiaate on mainio: se korvaa käyttöjärjestelmän oman COPY-käskyn ja suorittaa virustarkistuksen jokaiselle tiedostolle kopioinnin aikana. Tarkistus käy niin nopeasti, ettei HCOPY nopeudeltaan jää juurikaan jälkeen DOSin omasta kopiointikäskystä. Etsinnässä käytetyt sormenjäljet on saatu IBM:ltä ja ensimmäinen HCOPY-versio tunnisti niiden avulla 68 eri virusta.

Tarkoitus on, että käyttäjä nimeää HCOPYn uudelleen (esimerkiksi COBY.EXE) ja käyttää COBY-käskyä käyttöjärjestelmän COPYn sijaan. Näin virustarkistus tulee tehtyä automaattisesti ja lähes huomaamatta. HCOPY tuntee COPYn tapaan valitsimet /A, /B ja /V sekä korvausmerkit * ja ?, joten sen käyttö ei nimeä lukuunottamatta poikkea mitenkään COPYn käytöstä.

Jos HCOPY huomaa, että kopioitavassa tiedostossa on virus, se keskeyttää kopioinnin ja ilmoittaa viruksen nimen:

```
C:\>HCOPY A:PELI.EXE

A:\PELI.EXE may contain the 4096 virus.
Abort copying? (Y or N)
```

Kopiointi keskeytyy painamalla Y:tä jolloin HCOPY poistaa sen osan tiedostoa, joka on jo ehditty kirjoittaa levylle. Lopuksi HCOPY kysyy vielä, halutaanko myös alkuperäinen, viruksen sisältävä tiedosto poistaa:

```
Purge source file? (Y or N) N

0 files copied.
```

Tiedostoja voidaan kopioida myös tyhjälle (NUL) laitteelle, jolloin kopiota ei kirjoiteta mihinkään. Tämä mahdollistaa HCOPYn käytön tavallisen etsintäohjelman tapaan. Komento

```
C:\DOS>HCOPY *.* NUL
```

"kopioi" kaikki oletushakemiston tiedostot ja tarkistaa samalla niiden sisällön.

Muutama päivä messujen jälkeen McAfee laski liikkeelle oman, samalla periaatteella toimivan ohjelman ja antoi sille nimeksi VCOPY. Molemmat ohjelmat toimivat samalla tavalla ja eroavat toisistaan vain tuntemiensa virusten määrässä.

Muita etsintäohjelmia

Hollantilaista alkuperää oleva julkisohjelma VIRSCAN.EXE ei nimestään huolimatta ole mitään sukua IBM:n ohjelmalle. Tunnettujen virusten sormenjäljet luetaan etsinnän aluksi tiedostosta VIRSCAN.DAT. Sen jälkeen ohjelma tutkii käynnistyslohkon sekä kaikki COM, EXE, SYS, OVL ja BIN-tiedostot.

F-PROT -paketissa on omat ohjelmansa virusten etsimiseen levyiltä, tiedostoista ja keskusmuistista. Käynnistyslohko ja osiotaulukko voidaan tarkistaa F-DISINF-ohjelmalla, tavalliset tiedostot F-FCHK-ohjelmalla ja keskusmuisti F-SYSCHK-ohjelmalla. Kun F-FCHK huomaa tiedostoon tarttuneen viruksen, se kysyy "Disinfect?". Myönteisellä vastauksella ohjelma yrittää poistaa viruksen. Jos poisto onnistuu, ohjelma tulostaa "Cured...", muutoin "Virus could not be removed."

Viruskohtaiset torjuntaohjelmat

Edellä kuvattujen yleisten ohjelmien lisäksi on olemassa suuri joukko tiettyä virusta varten tehtyjä etsintä- ja tuhoamisohjelmia. Viruskohtaisia lääkkeitä on olemassa mm. Datacrimelle, Jerusalemille, Dark Avengerille, Ping-Pong -virukselle ja 1701:lle.

3. Tarkistussummaohjelmat

Vanhin ja yksinkertaisin tapa torjua viruksia perustuu tarkistussummien käyttöön. Siinä tutkimusohjelma kirjaa tietokantaansa kaikkien levyllä olevien ohjelmien nimet, pituudet, tekoajat sekä ohjelmatiedostojen sisällöstä lasketun tarkistussumman.

Yksinkertaisin mahdollinen tarkistussumma saadaan laskemalla kaikki ohjelmassa olevat bitit yhteen. Näin saatu yksittäinen luku on kuitenkin epäluotettava. Se ei esimerkiksi huomaa, mikäli kaksi konekielistä käskyä vaihdetaan keskenään. Huomattavasti luotettavampi summa saadaan, kun jokaisessa käskyssä otetaan huomioon myös sen sijainti. Tarkistussummien luotettavaan laskemiseen on vuosien varrella kehitetty useita erilaisia algoritmeja, joista ohjelman tekijä voi valita. Monet ohjelmat käyttävät kahta erilaista tarkistussummaa jolloin on täysin varmaa, että pieninkin tiedostoon tullut muutos huomataan.

Ohjelman toimintaa voidaan laajentaa niin, että se tarkistaa myös nollauran, osiotaulukon ja käynnistyslohkon sisällön. Keskeytysosoitteiden tarkistaminen lisää tehokkuutta, mutta saattaa aiheuttaa vääriä hälyytyksiä.

```
26210 12071        512 PARTITION-0:
25753  3050        512 PARTITION-1:
39458 58310        512 BOOTTRACK-C:
15632 22726      80592 C:\DOS\GWBASIC.EXE
35549 54003       3919 C:\DOS\FASTOPEN.EXE
32483  7984       3060 C:\DOS\NLSFUNC.EXE
17777 52837      11775 C:\DOS\REPLACE.EXE
43574 20139      11247 C:\DOS\XCOPY.EXE
 3228 60855       5825 C:\DOS\APPEND.EXE
55891 63867       3300 C:\DOS\GRAPHICS.COM
 5405 35687       2377 C:\DOS\LABEL.COM
29281 17465        313 C:\DOS\MORE.COM
21318 48989       9026 C:\DOS\PRINT.COM
20454 38090       4299 C:\DOS\RECOVER.COM
51746 34450      34643 C:\DOS\RESTORE.COM
12651 16586       3571 C:\DOS\TREE.COM
20482 53751      70711 C:\WORD5\MAKEPRD.EXE
50022 52299     622428 C:\WORD5\WORD.EXE
```

Check-it! kirjaa ohjelmat tietokantaansa. Pituuden lisäksi jokaisesta ohjelmasta lasketaan kaksi eri tarkistussummaa, jolloin kaikki tiedostoihin tehdyt muutokset tulevat varmasti ilmi.

Tarkistussummaan perustuvien ohjelmien hyvänä puolena on niiden kattavuus. Ne toimivat sellaisiakin viruksia vastaan, joista ohjelman tekijällä ei ole ollut aavistustakaan. Niitä on myös helppo tehdä. Vähänkin ohjelmointia tunteva harrastaja voi tehdä itselleen sopivan ohjelman Basicillä, Pascalilla tai C:llä. Ei ihme, että julkisohjelmien joukossa on lukematon määrä tällaisia ohjelmia huonosti tehtyinä.

Teoriassa olisi mahdollista tehdä virus, joka muuttaisi suoraan tarkistusohjelman käyttämää tietokantaa ja estäisi näin ohjelmiin tarttuneita viruksia näkymästä. Viruksen pitäisi kuitenkin tietää käytetyn tarkistussumman algoritmi ja tuntea tarkistusohjelman käyttämän tietokannan rakenne, joten mahdollisuus on todellakin vain teoreettinen.

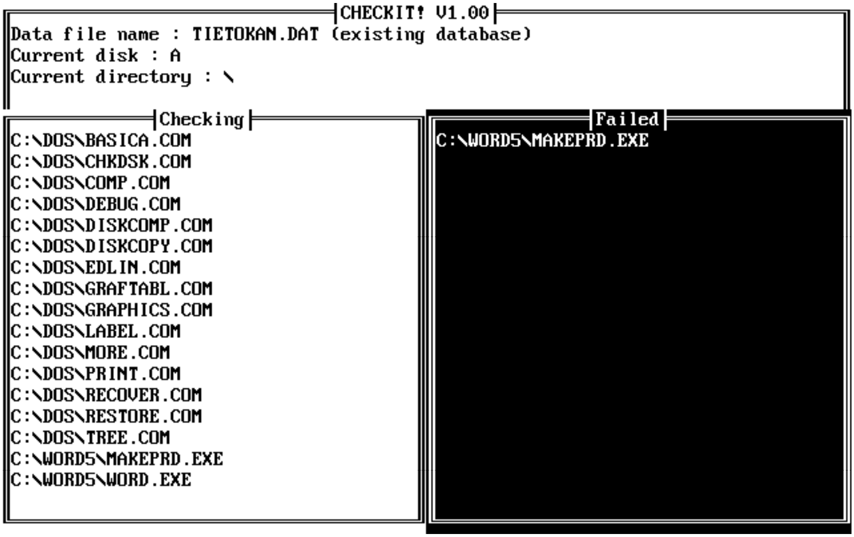
Hyvien puolien ohella tarkistussummilla on myös heikkoutensa. Isolla levyllä voi olla satoja ohjelmatiedostoja jolloin niiden tutkiminen, summien laskeminen ja tulosten vertaaminen tietokantaan kestää epäkäytännöllisen kauan. Tietokannan ylläpitäminen ohjelmien

kopioinnin ja poistamisen jälkeen on niin ikään työlästä, eikä tietokantaa voi kovinkaan helposti käyttää ohjelmalevykkeiden tarkkailuun. Lisäksi tarkistusohjelmat saattavat jopa levittää Dark Avengerin kaltaisia viruksia, koska ne tarttuvat jokaiseen tarkistussumman laskemista varten avattuun ohjelmatiedostoon. Moniajoon pystyvässä käyttöjärjestelmässä (kuten OS/2) summien laskennan ja vertailun voi hoitaa tausta-ajossa, jolloin se ei haittaa mikron normaalia käyttöä.

Kun tarkistussumma muuttuu, ohjelma antaa hälyytyksen ja kertoo muuttuneen tiedoston nimen. Ohjelma ei kuitenkaan kerro, mikä virus on kyseessä eikä osaa poistaa niitä. Ohjelmista ei ole myöskään apua tartunnan saaneiden levykkeiden jäljittämisessä eikä Troijalaisten torjunnassa.

Check-it!

Koska tarkistussumman laskeminen kuuluu osana moniin torjuntaohjelmiin ja koska sitä varten on saatavissa myös suuri joukko julkisoh-



Mikäli tarkistussummat eivät täsmää, Check-it! antaa varoituksen ja kertoo muuttuneen tiedoston nimen. Se ei kuitenkaan kerro, mitä tiedostolle on tapahtunut eikä mahdollisen viruksen nimeä.

jelmia, on tässä esitelty vain yksi kaupallinen tarkistussummaohjelma. Se on englantilaisen Zortechin tekemä Check-it! (huutomerkki kuuluu ohjelman nimeen).

Check-it! luo levykkeelle tietokannan, josta käyvät ilmi kiintolevyn ohjelmatiedostojen tarkistussummat. Käyttäjän on itse valittava mukaan otettavat tiedostot. Samalla lasketaan tarkistussumma osiotaulukosta ja käynnistyslohkosta sekä tallennetaan keskeytysosoitteet. Tarkistus käynnistyy komennolla CHECKIT! / .

Vaikka ohjelma tekeekin sen minkä lupaa, näyttää Check-it! jotenkin harrastelijamaiselta. Lisäksi siinä on eräitä suunnitteluvirheitä. Esimerkiksi kaikkien 256 keskeytysosoitteen tutkiminen tuottaa turhia varoituksia, sillä viimeiset osoitteet ovat käyttämättä ja saattavat sisältää satunnaisia arvoja.

Sentry

Sentry on McAfeen ohjelma, joka etsii viruksia tarkistussummien avulla. Ohjelman toimintaperiaate on kekseliäs: miksi turhaan laskea tarkistussumma koko tiedostosta, kun virus kiinnittyy lähes aina joko tiedoston alkuun tai loppuun? Ohjelmatiedoston alun ja lopun tutkiminen riittää lähes aina paljastamaan viruksen. Sentry käyttää tätä hyväkseen ja laskee tarkistussumman vain ohjelmatiedoston alusta, keskeltä ja lopusta, jolloin summien laskenta ja niiden vertaaminen käy erittäin nopeasti. Sentry on niin nopea, että sen voi lisätä AUTOEXEC.BATiin jolloin tiedostojen tarkistaminen tulee tehtyä aina käynnistyksen yhteydessä.

Tarkistussummien lisäksi Sentry vertaa keskeytysosoitteita ja antaa varoituksen jos niitä on muutettu. Ohjelman 2.0-versiossa varoitus annetaan vain yleisluontoisena eikä edes muuttuneen keskeytyksen numeroa kerrota. Tämä, samoin kuin tarkistussummien ylläpitoon liittyvät hankaluudet vähentävät ohjelman käytettävyyttä.

4. Muistinvaraiset torjuntaohjelmat

Muistinvaraiset torjuntaohjelmat jäävät muistiin virusten tavoin ja yrittävät sieltä käsin havaita mahdolliset virukset. Havaitseminen perustuu keskeytysten tarkkailuun.

Luvussa kaksi esitettiin, miten virus nappaa levytoimintoihin liittyviä keskeytyksiä itselleen ja pääsee niiden kautta vaikuttamaan koneen toimintaan. Keskeytysosoitetta ei voi muuttaa noin vain. Oikeaoppinen tapa osoitteen muuttamiseen on käyttää toista keskeytystä, yleiskeskeytyksen 21 palvelua 25, joka on lisätty DOSiin juuri tätä varten. Jos virusten torjuntaohjelma on napannut tämän keskeytyksen itselleen, se antaa hälyytyksen kun virus yrittää muuttaa minkä tahansa keskeytyksen osoitetta.

Toinen keskeytys, jota kannattaa tarkkailla, on numero 27 sekä saman asian paremmin hoitava 21-keskeytyksen palvelu 31. Ohjelmat käyttävät näitä keskeytyksiä silloin, kun ne haluavat jättäytyä keskusmuistiin. Virusten lisäksi keskeytystä käyttävät kaikki muistinvaraiset apuohjelmat, joista osa on DOSin omia. Tarkkailu voi siten tuottaa myös vääriä hälyytyksiä.

Muistinvarainen tarkkailuohjelma voi seurata myös aivan tavallisia levylle meneviä kirjoituspyyntöjä. Hälyytys annetaan eikä pyyntöä viedä loppuun asti, mikäli kutsussa annetut parametrit osoittavat esimerkiksi suoraa kirjoittamista varatuille alueille. Kutsut, joiden parametrit osoittavat viatonta toimintaa, päästetään tietenkin läpi sellaisinaan.

Muistinvaraiset ohjelmat eivät voi koskaan olla erityisen tehokkaita ja niiden toiminnassa on monia varauksia. Jotta vartiointiohjelma voisi edes teoriassa torjua viruksen, sen on päästävä muistiin tätä ennen. Koska käyttöjärjestelmään tai sen komentotulkkiin COMMAND. COMiin kiinnittyneet virukset pääsevät muistiin heti koneen käynnistyksen yhteydessä, ei vartiointiohjelma ehdi vaikuttaa niihin. Kun keskeytykset on jo ohjattu muualle, ei niiden tarkkailusta ole enää mitään hyötyä.

Uudet, entisiä kehittyneemmät virukset eivät edes käytä DOSin palveluita vaan ohittavat sen. Ne eivät muuta keskeytysosoitteita, vaan

selaavat keskusmuistin läpi, etsivät sieltä oikean palveluosoitteen ja kutsuvat suoraan sitä. Tällaista virusta on lähes mahdotonta havaita ohjelmallisesti.

Toisaalta muistinvaraiset vartijat ovat ainoita ohjelmia, joista on edes jonkinlaista apua troijalaisia vastaan.

Flushot Plus

Muistinvaraisista torjuntaohjelmista tunnetuin lienee ohjelma nimeltä Flushot Plus. Se on shareware-ohjelma, josta tekijä odottaa saavansa 10 dollarin korvauksen. Jos korvaus ohjelmointityöstä tuntuu liian suurelta, Ross M. Greenberg pyytää lähettämään 10 dollarin shekin, joka on osoitettu johonkin hyväntekeväisyystarkoitukseen sekä 4 dollarin shekin itselleen käsittelykulujen peittämiseksi. McAfeen tavoin Greenberg on taalansa ansainnut, sillä Flushot Plus on näppärä ja niin tehokas kuin muistinvarainen ohjelma ylipäätänsä voi olla. Flushotin 3-versio on itse troijalainen, joten sitä ei pidä käyttää.

Flushot koostuu kahdesta tiedostosta: ohjelmasta FSP.COM sekä datatiedostosta FLUSHOT.DAT. Kun FSP käynnistetään, se lataa itsensä pysyvästi keskusmuistiin. Työtila pienenee noin 16 kilotavulla.

Flushotin toimintaa säädellään FLUSHOT.DAT-tiedoston avulla. Aluksi se kopioidaan päähakemistoon, mutta sijaintia ja tiedoston nimeä voi myöhemmin muuttaa. Nimen muuttaminen ja tiedoston piilottaminen johonkin alihakemistoon estää viruksia ja trojalaisia löytämästä sitä. Koska FLUSHOT on muistinvaraisista ohjelmista tunnetuin, saattavat vahinko-ohjelmat pyrkiä huijaamaan sitä.

FLUSHOT.DAT koostuu riveistä, jolla kuvataan yksittäisille tiedostoille annetut asetukset. Mahdollisuuksia on viisi: P estää tiedostoon kirjoittamisen, R estää tiedoston lukemisen, E sallii P- ja R-määritysten kumoamisen yhdessä hakemistossa, T sallii ohjelman jäävän keskusmuistiin ja C laskee tiedostosta tarkistussumman. Näiden lisäksi on olemassa eräitä pienempiä, lähinnä toiminnan hienosäätöön tarkoitettuja asetuksia joita ei tässä yhteydessä käsitellä.

Ohjelman mukana tuleva FLUSHOT.DAT sisältää valmiiksi seuraavat rivit:

```
I=
P=*.bat
P=*.sys
P=*.exe
P=*.com
P=*FLUSHOT.DAT
R=*FLUSHOT.DAT
R=*AUTOEXEC.BAT
R=*AUTOEXEC.BAT
C=C:\COMMAND.COM[12345]
C=C:\IBMBIO.COM[12345]
C=C:\IBMDOS.COM[12345]
C=C:\IO.SYS[12345]
C=C:\MSDOS.SYS[12345]
```

P-asetuksilla estetään kirjoittaminen kaikkiin BAT, SYS, EXE ja COM-tiedostoihin. Ohjaustiedosto FLUSHOT.DAT on suojattu sekä lukua että kirjoittamista vastaan. AUTOEXEC.BATin kohdalla tekijälle lienee sattunut pieni erehdys, sillä nyt tiedosto on suojattu kaksi kertaa lukemista vastaan. Toisen R-kirjaimen tilalla pitäisi ilmeisesti olla P-kirjain.

Komentotulkki ja käyttöjärjestelmän kaksi piilotettua tiedostoa on suojattu tarkistussummalla. Summat lasketaan aina kun FSP ladataan muistiin. Koska ohjelman tekijä ei ole voinut tietää millainen DOS-versio käyttäjän koneessa on, hän on kirjoittanut hakasulkuihin vakioarvot 12345. Kun FSP käynnistetään ensimmäistä kertaa, saadaan virheilmoitus, joka kertoo summien poikkeavan FLUSHOT.DAT-tiedoston ilmoittamista. FSP kertoo uudet arvot, jonka jälkeen käyttäjän pitää korjata tiedoston arvot omaa tilannettaan vastaavaksi ja käynnistää FSP uudelleen. Jos DOS-versio käyttää tiedostoja IBM-alkuisia tiedostoja, poistetaan IO.SYSistä ja MSDOS.SYSistä kertovat rivit. Jos DOS-versio käyttää näitä, poistetaan vastaavasti IBMBIO- ja IBMDOS-rivit.

Merkkinä siitä, että FLUSHOT vartioi konetta, näkyy kuvaruudun oikeassa ylänurkassa '+' merkki. FSP:n vartiointi voidaan katkaista painamalla ALT-näppäintä kolme kertaa peräkkäin, jolloin merkiksi tulee '-'. Kolme painallusta palauttaa FSP:n jälleen toimintaan.

Kun FSP huomaa, että asetuksia rikotaan, se tulostaa ruudulle ikkunan. Esimerkiksi AUTOEXEC.BAT-tiedoston tulostaminen TYPE-käskyllä tuottaa seuraavan ilmoituksen:

```
Read Access being attempted on:
C:/AUTOEXEC.BAT
    (By The Command Line Interpreter)
Press "Y" to allow, "G" to go till exit, any other
key to exit.
```

Toiminto sallitaan painamalla Y:tä. Jos ajolupa halutaan antaa koko komennolle, painetaan G:tä. Minkä tahansa muun näppäimen painaminen keskeyttää toiminnon.

E-asetuksella voidaan suojaus kumota kokonaisesta hakemistosta tai sen osasta. Esimerkiksi rivi E=?\dev* poistaa vartioinnista kaikki \DEV-hakemistossa olevat tiedostot levyasematunnuksesta riippumatta.

Toinen FSP:n varoitusmekanismi tarkkailee ohjelmien tekemiä DOS-keskeytyksiä ja antaa varoituksen, mikäli se huomaa levyn alustamiseen tai suoraan levylle kirjoittamiseen liittyviä kutsuja. Esimerkiksi FORMAT A: -komento tuottaa ikkunan

```
====>Direct Disk Write attempt by program other than
DOS! <===
                 (From an Ioctl Call)
By: C:/DOS/FORMAT.COM
Press "Y" to allow, "G" to go till exit, any other
key to exit.
```

Suora kirjoittaminen levylle tuottaa ikkunan, josta näkyy käytetty keskeytys sekä kohteena oleva levyosoite:

```
====>Direct Disk Write attempt by program other than
DOS! <===
 Interrupt 26: =>Drive: A Head: 0 Track: 00000
Sector: 00001
```

```
By: C:/DOS/SYS.COM
Press "Y" to allow, "G" to go till exit, any other
key to exit.
```

Kolmas FSP:n suojakeinoista liittyy tarkistussummien laskemiseen. Jos summa on laskettu ja kirjoitettu FLUSHOT.DAT-tiedostoon, käy FSP tarkistamassa summan aina kun ohjelma ladataan muistiin. Ellei summa täsmää, tulostuu ikkunaan varoitus.

C-merkillä alkavalla rivillä voidaan suojata vain ohjelmatiedostoja. Käynnistyslohko voidaan ottaa mukaan tarkkailuun kirjoittamalla FLUSHOT.DAT-tiedostoon rivi

```
B=C12345
```

missä B tarkoittaa käynnistyslohkoa, C tarkoittaa C: asemaa ja 12345 tarkistussummaa. Kun B-asetus on tehty, FSP käy laskemassa käynnistyslohkon tarkistussumman aina käynnistyksensä yhteydessä.

Neljäntenä ja viimeisenä suojakeinona FSP pyrkii estämään ohjelmia jättäytymästä muistiin. Jos tällainen yritys havaitaan, ruudulle tulostuu varoitus:

```
? WARNING! TSR Request from an unregistered program!
Number of paragraphs of memory requested (in
decimal) are:00394

             (Press any key to continue)
```

Vartiointi voidaan poistaa niiltä ohjelmilta, joiden tiedetään jäävän muistiin, kirjoittamalla niiden nimet T-merkin jälkeen. Esimerkiksi rivit

```
T=C:\DOS\GRAPHICS.COM
T=C:\DOS\FASTOPEN.EXE
```

kertovat FSP:lle, että GRAPHICS ja FASTOPEN ovat hyväksyttäviä muistinvaraisia ohjelmia ja saavat jäädä muistiin halutessaan.

Pari yleisintä virusta FSP tuntee suoraan nimellä. Yritys ajaa Jerusalemilaisen saastuttama CHKDSK-ohjelma tuottaa ikkunan

```
An Attempt is being made to infect your system by:
PLO Virus (aka Jerusalem or Israeli Virus).
By: C:\DOS\CHKDSK.COM
Press "Y" to allow, "G" to go till exit, any other
key to exit.
```

jolloin virustartunta on helppo havaita.

FSP ei yksinään riitä suojaamaan mikroa viruksilta, mutta se täydentää mukavasti muiden ohjelmien antamaa suojaa. Koska ohjelman käyttö ja sen toimintaparametrien asettelu edellyttää jonkin verran asiantuntemusta, ei FSP sovellu aloittelijalle.

Mace Vaccine

Mace Vaccine on yksi monista Mace Utilities-apuohjelmapakettiin kuuluvista ohjelmista. Aiemmin ohjelmaa myytiin myös erikseen. Nimestään huolimatta sillä ei ole mitään tekemistä varsinaisten rokotusohjelmien kanssa. Vaccine on muistinvarainen tarkkailuohjelma, joka pyrkii estämään levyn sotkemisen ja suoran kirjoittamisen levylle. Jos kirjoitusta yritetään, kuvaruudun yläreunaan tulostuu punainen laatikko, jossa ohjelma kertoo mitä on tekeillä. Käyttäjä voi antaa kirjoituksen tapahtua tai estää sen. Grafiikkatilassa laatikon sijasta kuuluu äänimerkkinä Beethovenin 5. sinfonian kohtaloteema. Vaccinen lataaminen muistiin vähentää käytettävissä oleva RAMia reilulla kuudella kilolla.

Vaccine ladataan muistiin kirjoittamalla

```
C> VACCINE n
```

missä n on halutun suojaustason numero. Tasot on numeroitu yhdestä kolmeen ja tasoa voi muuttaa käytön aikana.

Ensimmäisellä tasolla (n=1) ohjelma estää muita kuin DOSia itseään kirjoittamasta FATiin ja loogisten levyasemien päähakemistoihin. Kirjoittaminen osiotaulukkoon, COMMAND.COMiin ja käyttöjär-

jestelmän piilotettuihin tiedostoihin sekä levykkeiden alustaminen on myös estetty.

Toisella tasolla suojaus laajenee siten, että mikä tahansa suora kirjoitusyritys levylle estetään. Tällaisia ovat mm. CHKDSK /F-valitsinta käytettäessä, Nortonin, Macen ja PC-Toolsin levyeditorit sekä pirstoutumisen poistoon tarkoitetut apuohjelmat.

Kolmas taso löytyy vain uudemmista Vaccine-versioista. Tällä tasolla ajettuna Vaccine laskee jokaisesta ajettavasta ohjelmasta tarkistussumman ennen sen käynnistämistä ja vertaa summaa tietokantaansa. Jos summa on muuttunut, tästä annetaan varoitus ja ohjelma ajetaan vasta käyttäjän annettua siihen luvan.

Tietokanta luodaan SURVEY-ohjelmalla. Se etsii kaikki levyllä olevat ohjelmatiedostot ja kirjoittaa HELP.CRC-nimisen tietokannan levyn päähakemistoon.

Vaccinen voi kytkeä hetkeksi pois päältä kirjoittamalla VACCINE OFF. Ellei näin tehdä, saattavat kiintolevyn testi- ja pakkausohjelmat toimia virheellisesti tai tuottaa jatkuvia varoituksia. Se kannattaa tehdä

```
╔════════════════════════[Mace VACCINE]════════════════════════╗
║ FFIND.EXE    is about to be executed. It has been altered    ║
║ since the survey program was last run. If this program       ║
║ is not self-modifying, it should be re-loaded from a master. ║
║ Type Y to allow this operation, N to disallow it, or X to    ║
║ disable all protection.                                      ║
╚═════════════════════[Protection Level = 3]═══════════════════╝
DBLOGM   FIX      4000  15.12.89  12.00
DESTROY  EXE      7004  15.12.89  12.00
FORMATH  EXE     48438  15.12.89  12.00
ICECREAM DBF      2162  15.12.89  12.00
MKEYRATE EXE     12913  15.12.89  12.00
REBOOT   EXE      2753  15.12.89  12.00
UNFORMAT EXE     56546  15.12.89  12.00
SORTD    EXE     45308  15.12.89  12.00
SQZD     EXE     43318  15.12.89  12.00
PARK     EXE     20004  15.12.89  12.00
SETPOP   EXE     48945  15.12.89  12.00
POP      EXE     14256  15.12.89  12.00
SURVEY   EXE     60014  15.12.89  12.00
VACCINE  EXE     13152  15.12.89  12.00
       40 File(s)   1101824 bytes free

D:\MACE>ffind
```

Mace Vaccine pyrkii estämään vahingolliset levyoperaatiot. Haluttaessa se myös tarkistaa jokaisen käynnistettävän ohjelman ja vertaa tarkistussummaa tietokantaansa. Jos summat eivät täsmää, annetaan käyttäjälle varoitus.

myös ennen Windowsin käynnistämistä. Vartiointi otetaan takaisin käyttöön kirjoittamalla VACCINE ON.

Levykkeet voi jättää vartioinnin ulkopuolelle kirjoittamalla VACCINE NF (no floppy). Näin kannattaa tehdä esimerkiksi silloin kun alustetaan joukko uusia levykkeitä.

F-DRIVER

F-DRIVER.SYS on F-PROT-ohjelmapaketin mukana toimitettava laiteohjain. Se asennetaan muiden ohjainten tavoin CONFIG.SYS-tiedostoon:

```
DEVICE=C:\FPROT\F-DRIVER.SYS
```

Aina, kun mikro käynnistetään, ohjain tarkistaa käynnistyslohkon ja antaa varoituksen, mikäli se havaitsee viruksen. Mikron käytön aikana F-DRIVER tarkistaa McAfeen Scanresin tavoin jokaisen käynnistettävän ohjelman. Jos ohjelmasta löytyy virus, F-DRIVER kertoo viruksen nimen ja estää ohjelman käynnistämisen.

Esimerkiksi yritys käynnistää Jerusalem-viruksen saastuttama CHKDSK-ohjelma tuottaa virheilmoituksen

```
C:\DOS>CHKDSK
This program is infected with the Jerusalem virus.
Access denied
```

eikä ohjelma käynnisty. DOSin tulostama ilmoitus "Access denied" kuuluu suomenkielisessä DOS-versiossa "Käyttöä ei sallita", joka sopii tilanteeseen paremmin kuin hyvin.

Koska vartiointi on tehty laiteohjaimen avulla, on se pelkkiä muistinvaraisia apuohjelmia tehokkaampi. F-DRIVER pääsee muistiin ennen sovelluksia jo käyttöjärjestelmän latauksen yhteydessä. Toinen F-DRIVERin hyvistä puolista on sen pieni muistinkulutus: ohjain vie alle kolme kilotavua keskusmuistia, mutta tuntee silti 99% viruksista suoraan nimeltä.

TSAFE

TSAFE on Turbo Anti-Virus -paketin muistinvarainen apuohjelma. Se vie noin 20 kilotavua keskusmuistia. Ohjelma estää haluttaessa levykkeiden ja kiintolevyn alustamisen, niille kirjoittamisen ja ohjelmien jäämisen keskusmuistiin. TSAFE-ohjelmaa ei ole kopiosuojattu.

Kirjoitussuoja kiintolevylle

Kirjoitussuojan asettaminen levykkeelle estää viruksia tarttumasta itse levykkeeseen tai siinä oleviin ohjelmiin. Valitettavasti suojausta ei voi käyttää kiintolevyillä, sillä kirjoitussuojakytkin löytyy vain harvoista kiintolevyistä.

Kiintolevyn kirjoitussuojaa voidaan jäljitellä ohjelmallisesti, joskaan tällainen suojaus ei ole koskaan fyysisen suojauksen veroinen. Ohjelma voisi teoriassa kiertää suojauksen ohittamalla DOSin ja ohjaamalla suoraan kiintolevyn ohjainkorttia. Suojaukseen on saatavilla useita julkisohjelmia. Asian hoitaa tekee myös FPROT-paketin F-DLOCK.

Kirjoitussuojaa ei tietenkään voi käyttää jatkuvasti. Se kannattaa kytkeä päälle vain silloin, kun ajetaan uutta, ennestään tuntematonta ohjelmaa, jonka ei pitäisi kirjoittaa levylle mitään.

5. Tutkimisohjelmat

Tutkimisohjelmat pyrkivät selvittämään ohjelmatiedoston toimintaa lukemalla sen suoraan levyltä normaalin tiedoston tavoin ja analysoimalla ohjelmasta löytyviä konekielikäskyjä.

Tutkimisohjelman käytössä on monia rajoituksia. Ohjelma ei voi varmasti tietää, mikä kohta tutkittavasta koodista on dataa ja mikä varsinaista ohjelmakoodia, koska kaikki bitit ovat saman näköisiä. Bittien lopullinen merkitys selviää vasta tavasta, jolla niitä tulkitaan. Esimerkiksi kuvan kohdalla käytetyt bitit saattavat näyttää vaikka

kuinka vaaralliselta ohjelmakoodilta, jos niitä yritetään tulkita ohjelmana.

Silloinkin, kun tiedetään tutkittavan kohdan olevan varmasti ohjelmakoodia, on käytettyjen DOS-palveluiden jäljittäminen vaikeata. INT-komennot löytyvät koodin seasta kohtuullisen helposti, mutta samalla keskeytyksellä voidaan rekisterien arvoista riippuen tehdä useita erilaisia asioita. Rekisterien arvot saatetaan asettaa aliohjelmassa, joka sijaitsee aivan toisessa kohtaa, tai ne saattavat olla tuloksia laskutoimituksista. Tästä syystä analysointiohjelmat eivät pysty tutkimaan ohjelman toimintaa kovinkaan tarkasti. Täysin luotettava analyysi ohjelman toiminnasta saataisiin vain ajamalla se.

Koodianalyysin lisäksi tutkimisohjelmat tulostavat myös ohjelmakoodista löytämänsä selväkieliset merkkijonot. Osa teksteistä on virheilmoituksia, jotka kääntäjä on lisännyt ohjelmaan muuntaessaan

```
torus2.exe                                                   Hex format
 Cluster 315, Sector 346                      File offset 73 216, hex 11E00
2A001000 7606633A 5C626273 5C66696C 65735C2A 2E2A1000 █.►.v♠c:\bbs\files\*.*►.
8A06633A 5C626273 5C6D656E 75735C2A 2E2A1100 9E06633A è♠c:\bbs\menus\*.*◄.₧♠c:
5C626273 5C6D6169 6E5C6675 636B2E0A 1C00B406 20486161 \bbs\main\fuck.◙∟.┤♠ Haa
612E2E2E 20476F74 20796F75 2E2E2E2E 2E2E2E2E 2E2E2E2E a... Got you............
0C00D406 633A5C62 62735C66 75636B2E 1200E406 633A5C62 ♀.╘♠c:\bbs\fuck.↕.Σ♠c:\b
62735C66 696C6573 5C667563 6B2E0600 FA06633A 5C2A2E2A bs\files\fuck.♠.·♠c:\*.*
07000407 696E692E 62617400 12001007 666F726D 61742063 •.♦•ini.bat.↕.►•format c
3A203C63 72203E6E 756C0200 26076372 01002C07 59310000 : <cr >nul☻.&•cr☺.,•Y1..
40400300 36075945 53000B00 3E074361 6C63756C 6174696E @@♥.6•YES.♂.>•Calculatin
67F40700 4E07536F 7274696E 67F40000 803F0000 5E070400 g⌠•.N•Sorting⌠..Ç?..^•♦.
62073132 42440500 6A073132 37383902 02007407 31320100 b•12BD♣.j•12789☻☻.t•12☺.
7A074122 01008007 33222F00 8607536F 7272792E 20477261 z•A"☺.Ç•3"/.å•Sorry. Gra
70686963 73206E6F 74206176 61696C61 626C652E 2043616E phics not available. Can
27742072 756E2054 6F727573 2E200D00 BA074F75 74206F66 't run Torus. ♪.║•Out of
206D656D 6F727922 1400CC07 52656475 63696E67 2070616E  memory"¶.╠•Reducing pan
656C7320 66726F6D 0200E407 746F1600 EA075265 64756369 els from☻.Σ•to▬.Ω•Reduci
6E672073 65637469 6F6E7320 66726F6D 08000408 31323738 ng sections from◘.♦◘1278
39424344 24001008 5550202E 2E2E2E2E 2E2E2E2E 2E2E2E2E 9BCD$.►◘UP ............
2E204D6F 76652074 6F206E65 78742066 69656C64 24003808 . Move to next field$.8◘
444F574E 202E2E2E 2E2E2E2E 2E204D6F 76652074 6F207072 DOWN ........ Move to pr
6576696F 75732066 69656C64 24006008 4C454654 202E2E2E evious field$.`◘LEFT ...
2E2E2E2E 2E2E2052           Press Enter to continue    ...... R
1Help  2Hex  3Text  4Dir  5FAT  6Partn  7  8Choose  9Undo  10QuitNU
```

TORUS2.EXE on troijalainen, joka on kiertänyt purkeissa myös nimellä NEWTORUS.LZH. Grafiikkademon jälkeen ohjelma tuhoaa mm. levyn päähakemiston. Ohjelman lopusta löytyvät mm. tekstit "fuck" ja "Got you" joiden pitäisi soittaa hälyytyskelloja. Mutta kukapa viitsisi tutkia ohjelman ennen kuin kokeilee sen ajamista?

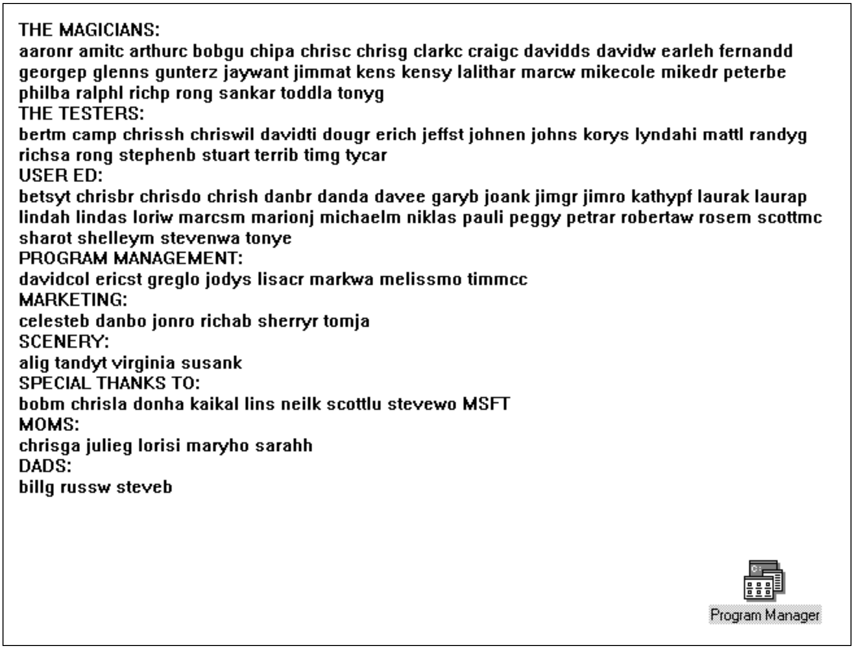
sen konekielelle. Loput tekstit ovat ohjelmoijan kirjoittamia ja tulostuvat eri kohdissa ohjelmaa. Jos ohjelmasta löytyy "Fuck you!" tai "Arf, arf, got you!" kaltaisia tekstejä, on ohjelma todennäköisesti Troijan hevonen ja se on viisainta jättää ajamatta. Viruksista vain harvat (kuten Disk Killer ja Dark Avenger) sisältävät selväkielisiä tekstejä.

Tekstit, joita ohjelma tulostaa, on erittäin helppo piilottaa. Esimerkiksi useimpien virusten tulostamat viestit on salakirjoitettu niin, etteivät ne näy suoraan ohjelmatiedostoa tutkimalla. Tästä syystä tekstien puuttuminen ei riitä takaamaan ohjelman vaarattomuutta.

Kaupallisissa ohjelmissa olevien viestien tutkiminen saattaa tuottaa huvittaviakin tuloksia. Esimerkiksi DOS 2.0:n RECOVER-apuohjelmasta löytyivät tekstit "Microsoft rules ok" ja "Chris Peters helped with the new dos!". Ne tulostuivat ruudulle jos käyttäjä painoi Ctrl-W:tä ohjelman pyytäessä kuittausta. Uudemmista DOS-versioista ilmoitukset on poistettu. AST:n muistiohjaimista REMM.SYS ja REX.SYS löytyi puolestaan teksti "Len Galasso was here!" Ohjainten tekijä oli halunnut jättää puumerkin työhönsä.

```
 Sector 277-278 ══════════════════════════════════════════ Hex format
 Cluster 134, Sector 277                                 Offset 0, hex 0
52524543 542A2A2A 0D0A4F6E 65206F66 20746865 204D6963 RRECT***♪◙One of the Mic
726F736F 66742057 6F726420 6C6F6164 2066696C 65732063 rosoft Word load files c
616E6E6F 740D0A62 6520636F 72726563 746C7920 72656164 annot♪◙be correctly read
2E0A0D24 0D0A2A2A 2A4E4F4E 2D434F50 59205052 4F544543 .◙♪$♪◙***NON-COPY PROTEC
54454420 4449534B 2A2A2A0D 0A546869 73206469 736B2069 TED DISK***♪◙This disk i
73206E6F 7420636F 70792070 726F7465 63746564 2C20796F s not copy protected, yo
750D0A63 616E206D 616B6520 6261636B 75702063 6F706965 u♪◙can make backup copie
73206F66 20746869 73207072 6F677261 6D0D0A6F 6E6C7920 s of this program♪◙only
77697468 20746865 20737570 706C6965 64207574 696C6974 with the supplied utilit
6965732E 0D0A240D 0A2A2A2A 494E5445 524E414C 20534543 ies.♪◙$♪◙***INTERNAL SEC
55524954 59205649 4F4C4154 494F4E2A 2A2A0D0A 54686520 URITY VIOLATION***♪◙The
74726565 206F6620 6576696C 20626561 72732062 69747465 tree of evil bears bitte
72206672 7569742C 0D0A6372 696D6520 646F6573 206E6F74 r fruit,♪◙crime does not
20706179 2E0D0A20 20202020 20205448 45205348 41444F57  pay.♪◙      THE SHADOW
204B4E4F 57530D0A 0A0A0A0A 0A0A0A0A 0A0A0A0A 0A0A0A0A  KNOWS♪◙◙◙◙◙◙◙◙◙◙◙◙◙◙◙◙◙◙
54726173 68696E67 2070726F 6772616D 20646973 6B2E0D0A Trashing program disk.♪◙
24A10501 FF060501 50CD1158 59415150 B82A00CD 1259C39C $í♣☺.♠♣☺P=◄XYAQP╕*.=↕Y├£
48FD03F9 03F14E4F 5053A3CC 08FF0ECC 0875075B 58A3CC08 H²♥·♥±NOPSú╠◘.♫╠◘u•[Xú╠◘
50538B17 B85562F7 E2051936 90890743 8AD0AC32 C2AAE2DD PSï↨╕Ub≈Γ♣↓6Éë•Cè╨¼2┬¬Γ▌
585B9DC3 0000FFFF 5A3A5C4D 53544F4F 4C535C4D 572E434F X[¥├....Z:\MSTOOLS\MW.CO
4D00FF00 00000000 07004D57 20202020 2020434F 4D000000 M.......•.MW      COM...
00000000 00000000          Press Enter to continue    ........
1Help  2Hex  3Text  4Dir  5FAT  6Partn  7  8Choose  9Undo  10QuitNU
```

Microsoft Word 2.0:n ohjelmakoodi sisälsi ylimääräisiä tekstejä, joiden tarkoituksena oli ilmeisesti vain peloitella laittomien kopioiden tekijöitä.



Windows 3:n tekijät ovat ikuistaneet sähköpostinimensä ohjelmaan. Nimet saa näkyviin pienellä niksillä.

Kaikkea muuta kuin huvittavia tekstejä löytyi Microsoftin Word 2.0:n ohjelmalevykkeiltä. Ohjelma oli vuonna 1985 ilmestyessään kopiosuojattu ajan hengen tapaan. WORD.COM-tiedoston lopusta löytyivät mm. tekstit "Trashing program disk", "Crime does not pay" ja "Shadow knows". Tekstit liittyivät kopiosuojauksiin ja niiden tarkoituksena oli ilmeisesti pelotella niitä, jotka aikoivat poistaa ohjelman suojauksen. Mitään levyä tuhoavaa (trashing) osuutta ohjelmasta ei koskaan löydetty. Tällaisen lisääminen olisikin ollut Microsoftilta perin arveluttavaa politiikkaa.

Windows 3.0:ssa tekijöiden nimet saa näkyviin painamalla F3-näppäimen pohjaan, kirjoittamalla WIN3, vapauttamalla F3:n ja painamalla lopuksi Backspace. Windowsin taustalle syttyvät tekijöiden nimet alueensa mukaisesti ryhmiteltyinä. Kohdasta "DADS" ("isukit")

löytyy nimi billg, joka tarkoittaa Bill Gatesia, Microsoftin perustajaa, toimitusjohtajaa ja alan tärkeintä vaikuttajaa.

Parhaimmaksi ovat kuitenkin pistäneet Ami-tekstinkäsittelyohjelman tekijät, sillä he ovat lisänneet ohjelmakoodiin omat kuvansa! Tekijät saadaan näkyviin katsomalla ohjelmaa Windowsin EXERAY-läpivalaisuohjelmalla. EXERAY on Windows-ohjelmien analysointiin tarkoitettu apuohjelma. Se näyttää tutkittavan ohjelman käyttämät resurssit, joita ovat mm. erilaiset osoitintyypit ja bittikarttakuvat. Mikään virusten etsintäohjelma se ei ole.



Koska tutkimusohjelmat analysoivat ohjelman koodia, ne voivat havaita sekä viruksia että Troijan hevosia. Teknisten rajoitusten vuoksi ohjelmien toimivuus ei koskaan voi olla täysin 100-prosenttista.

CHK4BOMB

CHK4BOMB ("Check for bombs") oli eräs ensimmäisiä pommien ja troijan hevosten etsintään kehitetyistä julkisohjelmista. Se tehtiin aikana, jolloin PC-viruksista ei vielä tiedetty mitään.

Iästään huolimatta ohjelma on käyttökelpoinen vielä tänäänkin. Se tulostaa ruudulle kaikki ohjelmakoodissa olevat merkkijonot sekä antaa lopuksi varoituksen, mikäli koodista löytyy vaarallisia DOS- tai BIOS-kutsuja ja näyttää osoitteet, joissa näitä kutsuja tehdään.

Ohjelman tekemä analyysi on yksinkertainen ja suoraviivainen. Se laskee vain keskeytykset, joissa kirjoitetaan suoraan levyn pinnalle eikä se muutenkaan tunnista kuin muutaman vaarallisen kutsun. Tästä on tosin se etu, ettei ohjelma yleensä anna turhia varoituksiakaan.

```
C:\DOS>CHK4BOMB FORMAT.EXE

                 CHECK FOR BOMBS
   Written by: Andy Hopkins
               526 Walnut Lane
```

```
               Swarthmore, PA 19081
CHECKING 23243 BYTES

IBM DOS Version 4.00 (C)Copyright IBM Corp 1981,1988
Licensed Material - Program Property of IBM
/SELECT
/BACKUP
/AUTOTEST
...
x:\IBMBIO.COM
x:\IBMDOS.COM
NO NAME
...
 Viallisia sektoreita %1 tavua.
Kokonaislevytila %1 tavua.
Aseta uusi levyke asemaan %1:
rjestelm
 %1 tavua.
$Aseta levyke uudestaan asemaan %1:
 taltion nimi (enint
n 11 merkki
). -
...
End of File: 23244 bytes.

****WARNING****
This program uses the ROM BIOS routines for direct
disk access at the following locations.
CS:1361    CS:139D    CS:13F6    CS:1590    CS:16B0

This program COULD format a disk or write to certain
sectors without
updating the directory or File Allocation Table.

****WARNING****
This program writes to absolute sectors at the
following locations:
CS:5224
The possibility exists to overwrite important data!

10/29/85 Andy Hopkins
```

DOS 4.0:n FORMAT-ohjelma alustaa levyn ja käyttää muitakin suoria kirjoituskäskyjä. Ohjelman käyttämät keskeytykset tuottavat tästä syystä monia varoituksia. Näkyvissä on vain osa

CHK4BOMB-ohjelman tulostamista merkkijonoista. Niistä nähdään mm. mielenkiintoiset dokumentoimattomat valitsimet (/BACKUP, /SELECT, /AUTOTEST) sekä eräitä ohjelman käyttämistä virheilmoituksista. Ohjelma on katkaissut ilmoitukset Ä-kirjainten kohdalta koska se ei ole pitänyt niitä tekstimerkkeinä.

PROGNOSE

CHK4BOMB etsii ohjelmasta vain keskeytyksiä, jotka liittyvät suoraan levynkäyttöön joko lukemis-, kirjoittamis- tai alustustarkoituksissa. PROGNOSE-niminen julkisohjelma etsii kaikki keskeytykset, laskee niiden määrän ja tulostaa käytetyistä keskeytyksistä sanallisen kuvauksen. Kuvaus tuntuu aluksi hyvinkin vakuuttavalta, esittäähän ohjelma sen selväkielisenä ja asiantuntevasti. Vasta kun on tutkinut PROGNOSEn avulla useita ohjelmia huomaa, että jokaisella keskeytyksellä olevan oman vakioselityksensä.

PROGNOSE erittelee koodissa olevat DOS-kutsut pelkän INT-keskeytyksen numeron perusteella eikä se pysty erottelemaan mitä alipalvelua ohjelma kulloinkin käyttää. Esimerkiksi yleisin DOS-kutsu numero 21 käsitellään vain "keskeytysten keskeytyksenä" vaikka sillä voi tehdä yli 100 erilaista asiaa.

PROGNOSE ei pysty erottelemaan, mikä kohta ohjelmasta on koodia ja mikä dataa. Tämän vuoksi se näkee joskus keskeytyksiä sielläkin, missä niitä ei ole ja saattaa tästä syystä antaa vääriä tietoja.

PROGNOSE antaa ohjelmalle turvaluokituksen, joka riippuu sen käyttämien keskeytysten vaarattomuudesta. Edellä kuvatuista syistä johtuen tämä luokitus ei kuitenkaan ole järin luotettava.

```
C:\DOS>PROGNOSE FORMAT.COM

           +----------------------------------+
           | PROGNOSIS Program Interrupt Check |
           | Version 1.0                       |
           | Copyright <C> 1985       D. Haacke|
           | IBM PC Utilities      Billings, MT|
           +----------------------------------+
```

```
Reading File.........:FORMAT.COM

Safety Rating........: 10   0 is safest.

Diagnosis............:Use with Back-Ups only on
floppy-only machines
Possible Interrupts..:15



Press any key to see report...


The interrupts found were:

 01h 02h 03h 06h 08h 10h 13h 16h 19h 20h 21h 25h 26h
2Fh 8Bh

Press any key to see report...

                   PROGNOSIS for FORMAT.COM
 Page 2

Ah, the Program Terminate Interrupt 20h. Very
Common. Harmless.

Ah, the INTERRUPT OF INTERRUPTS 21h. It is used 99
times here.
It accesses many DOS services and has many uses.
Destructive calls can destroy File Allocation
Tables, although unlikely. It will be found
throughout most code that uses DOS.

This is the Absolute Disk Read Interrupt 25h. This
program wants to access disk information
no-matter-what. This is usually no biggie, but some
copy-protection schemes might use this. Reads legal
sectors.

*** W A R N I N G *** This is the Absolute Disk
Write Interrupt 26h.
The program is going to write to the disk without
using conventional methods.It could do all sorts of
damage to disks should it write over a file or File
Allocation Table. I suggest testing this on scratch
```

```
diskettes only in a system that doesn't have a hard
disk.

A total of 15 possible Interrupt Calls were found.
```

PROGNOSEn antama tulos FORMAT-ohjelmasta. FORMAT saa turvallisuusluokituksen 10 ja sen käyttöä suositellaan vain levykekoneissa. Tämän jälkeen PROGNOSE tulostaa ohjelmasta löytyneet keskeytykset sekä antaa niistä lyhyen kuvauksen. Vain kuvauksen jälkimmäinen sivu on näkyvissä. Varoitus annetaan keskeytyksestä numero 26, jolla voidaan kirjoittaa suoraan levyn pinnalle.

6. Tietoturvaohjelmat

Tietoturvaohjelmia ei ole suunniteltu pelkkään virustorjuntaan. Ne pyrkivät ottamaan kokonaisvastuun mikron turvallisuudesta ja suojaamaan sen niin viruksilta kuin laitevioiltakin.

Certus

Certus muodostaa paketin, johon kuuluu useita käytön valvontaan ja tiedostojen turvaamiseen tarkoitettuja apuohjelmia. Ohjelmat eivät ole erityisen käyttäjäystävällisiä joten Certuksen käyttö vaatii asiantuntemusta ja asiaan perehtymistä. Certus ei olekaan tavallisen loppukäyttäjän ohjelma. Eniten hyötyä siitä on suurissa yrityksissä, jolloin mikrotukihenkilö voi Certuksen asentamalla valvoa ja suojella mikroja entistä paremmin. Lähiverkkoja varten Certuksesta on saatavissa oma Certus Plus-versio.

Asennuksen yhteydessä Certus luo ns. kriittisen levykkeen. Asennusohjelma siirtää levylle käyttöjärjestelmän ja kopioi levykkeelle myös FATit, nollauran ja CMOS-paristovarmennetun muistin sisällön. Jos levy sekoaa tai CMOS-muistin sisältö nollautuu, voidaan kone käynnistää kriittisellä levykkeellä ja tiedot palauttaa takaisin koneeseen. Näin Certuksesta on apua myös tavallisen laite- tai levyvian sattuessa.

Kahden ohjelmalevykkeen lisäksi Certus-pakettiin kuuluu kolmaskin levyke, "Blue disk". Tämä levyke sisältää yli 6000 julkisohjelman

```
                          Tue Jun 19 09:00:13 1990
09:00 C:\CERTUS\FAT.EXE
09:00 C:\CERTUS\SURVEY.COM
09:00 C:\CERTUS\HISTORY.EXE

                          Tue Jun 19 09:47:50 1990

09:00 C:\DOS\KEYB.COM
09:00 C:\WINDOWS\CHKDSK.COM
09:02 A:\DIR100.EXE                         FAILED
09:47 C:\CERTUS\FAT.EXE
09:47 C:\CERTUS\SURVEY.COM
09:47 C:\CERTUS\HISTORY.EXE

                          Tue Jun 19 10:12:18 1990

09:47 C:\DOS\KEYB.COM
09:47 C:\NORTON\SCAN.EXE
09:56 C:\DOS\ATTRIB.EXE
09:58 A:\RBOOT.COM
10:06 C:\DOS\APPEND.EXE
10:07 C:\DOS\CHKDSK.COM
10:07 C:\CERTUS\SHELTER.EXE
10:07 C:\CERTUS\SECURE.EXE
10:08 C:\COMMAND.COM
10:08 C:\CERTUS\QUICK.EXE
10:08 C:\CERTUS\SECURE.EXE
```

Certus pitää haluttaessa kirjaa kaikista koneessa ajetuista ohjelmista. A: asemalta käynnistetyn DIR100-ohjelman ajo on estetty, koska sitä ei ole lueteltu Certuksen hyväksymien sovellusten listalla.

nimet ja niistä lasketut tarkistussummat. Vertaamalla omia ohjelmiaan listan antamiin tietoihin käyttäjä voi vakuuttua siitä, että ohjelma on kunnossa ja ettei siihen ole tehty asiattomia lisäyksiä (kuten virusta tai jälkikäteen lisättyä Troijan hevosta).

Certus pystyy pitämään kirjaa koneessa olevien ohjelmien käytöstä. Ajetun ohjelman nimi, kellonaika ja muita tietoja tallennetaan haluttaessa lokitiedostoon. Tiedostosta on apua mm. silloin, kun koneesta löytyy virus ja halutaan jäljittää ohjelma, jonka mukana se on päässyt koneeseen.

Tärkeimmät Certus-paketin ohjelmista ovat:

QUICK: ylläpito-ohjelma, joka luo tietokannan levyllä olevista ohjelmista, laskee niistä tarkistussummat ja mahdollistaa tiedostomääreitten muuttamisen.

SURVEY: pieni muistinvarainen ohjelma, joka pyrkii estämään suorat kirjoitukset varatuille alueille ja haluttaessa myös tiedostojen kopioinnin levykkeille. Näin voidaan estää mikrossa olevien ohjelmien ja tiedostojen varastaminen.

RESIDENT: muistinvarainen ohjelma, joka tarkistaa sovellukset käynnistyksen yhteydessä ja antaa varoituksen, mikäli ohjelmatiedostoa on muutettu. Haluttaessa RESIDENT estää muiden kuin tietokantaan määriteltyjen ohjelmien ajamisen.

SHELTER: luo ja päivittää kriittistä levykettä sekä estää kiintolevyä näkymästä. Kun levy ei näy, ei sille voi kirjoittaa eikä kopioida mitään. Suojaus voi olla hyödyllinen silloin kun koneessa testataan ennestään tuntematonta ohjelmaa, jonka ei haluta vahingoittavan kiintolevyä.

KEYBD.SYS: laiteohjain, joka CONFIG.SYSiin asennettuna estää käyttäjää keskeyttämästä alkulatausta ennen kuin Certuksen ohjelmat on saatu ladattua muistiin.

KILLFILE: poistaa tiedoston niin, ettei sitä pysty palauttamaan (kuten Nortonin Wipefile).

Watchdog

Fischer International Systems Corporation on erikoistunut tietoturvaan ja tietojen salaamiseen. Tuotevalikoimaan kuuluu mm. erilaisia DES- ja RSA-salaustuotteita isoille IBM-keskuskoneille sekä PC:lle tarkoitettu Watchdog, jonka ensimmäinen versio julkistettiin jo vuonna 1983.

Watchdog (suom. vahtikoira) pyrkii luomaan mikroon minikonemaisen käyttöympäristön. Käyttäjille annetaan tunnukset ja salasanat, jotka kysytään aina mikron käynnistämisen yhteydessä. Kunkin käyttäjän tiedot tallentuvat käyttöprofiiliin (user profile). Profiiliin voidaan myös luoda käyttäjäkohtainen AUTOEXEC.BAT-tiedosto, joka käynnistää halutun ohjelman. Erityisen käyttökelpoinen Watchdog on

silloin, kun yhdellä mikrolla on useita eri käyttäjiä. Yhdelläkin käyttäjällä Watchdogista on hyötyä: se takaa, ettei kukaan muu pysty käyttämään levyllä olevia ohjelmia ja tiedostoja.

Pääkäyttäjä, System Administrator, jakaa levyllä olevat hakemistot eri käyttäjille ajo- , luku- , kirjoitus- ja luonti/poisto-oikeuksin. Tiedostot voidaan haluttaessa koodata salakielelle, jolloin tiedostoja voi käyttää vain niiden alkuperäinen tekijä. Työtiedostojen salakirjoitus tapahtuu lennossa siten, ettei se vaikeuta sovellusten käyttöä. Hakemistojen lisäksi voidaan rajoittaa sarja- ja rinnakkaisporttien sekä eri levyasemien käyttöoikeutta. Myös aloitustiedostojen (CONFIG.SYS ja AUTOEXEC.BAT) muuttaminen voidaan estää. Eri käyttäjien yhteiset ohjelmat voidaan koota kirjastoiksi, jolloin niitä ei pysty kopioimaan eikä muuttamaan. Tämä suojelee käyttäjiä myös viruksilta.

Tiedot eri ohjelmien käytöstä kellonaikoineen tallentuvat lokiin, josta tiedot voidaan tulostaa ulos erilaisina raportteina. Lokiin kirjautuvat myös System Administratorin tekemät asetukset sekä oikeustasojen rikkomisyritykset.

Watchdogiin kuuluu muistinvarainen vartijaohjelma, joka yrittää estää suorat kirjoitusyritykset levyn kriittisille alueille. Kirjastoidut ohjelmat tarkistetaan säännöllisesti, eikä niitä ajeta lainkaan mikäli ohjelmaan on tehty muutoksia.

Koneen sisälle asennettava lisäkortti (Watchdog Armor) parantaa tietoturvaa entisestään. Se estää mikron käynnistämisen A: asemassa olevalla levykkeellä ja suorittaa salakirjoittamisen elektroniikan avulla. Kortilla oleva kello toimii PC:n kellosta riippumatta ja takaa luotettavat lokitiedot.

7. Muut torjuntaohjelmat

Edellä lueteltujen ryhmien ulkopuolelle jää joukko ohjelmia, jotka on tarkoitettu tiedostojen rokottamiseen, levyn varattujen alueiden näyttämiseen ja havaittujen virustartuntojen poistamiseen.

Rokotusohjelmat

Rokotteiksi kutsutaan ohjelmia, jotka tekevät tiedostoista immuuneja tietyille viruksille. Tämä tapahtuu sijoittamalla ohjelmaan tunnus, jota virus itsekin käyttää. Nähdessään tiedostossa olevan tunnuksen virus luulee jo tartuttaneensa tiedoston ja jättää sen rauhaan.

Esimerkki rokotusohjelmasta on F-PROT-paketin mukana tuleva F-INOC. Se rokottaa kokonaisia levykkeitä Pakistanilaista ja Italialaista virusta vastaan kirjoittamalla näiden käyttämän merkin levykkeen käynnistyslohkoon.

Rokotusohjelmien käyttö on jokseenkin kyseenalaista. Miksi tyytyä rokottamaan tiedostoja virusten varalta kun paljon mielekkäämpää olisi poistaa virus järjestelmästä kokonaan?

Näyttöohjelmat

Näyttöohjelmat tulostavat kuvaruudulle käyttöjärjestelmän varattujen alueiden sisällön, joihin käyttäjä ei muuten pääse kurkistamaan. Tällaisia ohjelmia ovat mm. F-PROT -paketin F-BOOT (tulostaa käynnistyslohkon) ja F-PBR (tulostaa osiotaulukon). Ohjelmia voi käyttää, ellei omista yleiskäyttöistä levyeditoria, jolla voi katsoa ja muuttaa mitä tahansa levykohtaa. Ruudulle tulostuvan tekstin tulkinta vaatii jonkin verran asiantuntemusta. Viruksen erottaa usein siitä, että se on korvannut alkuperäiset selväkieliset virheilmoitukset omalla konekielisellä koodillaan.

Clean

Clean on McAfeen tekemä puhdistusohjelma. Jos Scan-ohjelma löytää levyltä viruksia, voidaan tiedostot puhdistaa Cleania käyttäen. Puhdistus tapahtuu Scan-ohjelman ilmoittaman koodin perusteella. Esimerkiksi Scanin antama ilmoitus

```
Scanning C:\DOS\CHKDSK.COM
  Found Jerusalem Virus Version B [Jeru]
```

kertoo Jerusalem-viruksen tarttuneen CHKDSK-ohjelmaan. Hakasuluissa näkyy Scan-ohjelman viruksesta käyttämä koodi. Tästä koodista Clean tietää, mikä virus sen pitää poistaa.

Viruksen poistaminen tehdään kirjoittamalla

```
C:\DOS>CLEAN CHKDSK.COM [Jeru]
CLEAN 2.1V55 Copyright 1989 by McAfee Associates.
(408) 988-3832
Cleaning [Jeru]
Scanning C:CHKDSK.COM
  Found Jerusalem Virus Version B [Jeru]
  Virus removed.

Found 1 file containing a virus.
1 virus were removed.
```

Useita tiedostoja, hakemisto tai koko levy voidaan puhdistaa kerralla antamalla tiedostonimen kohdalla hakemiston nimi tai levyasematunnus.

Clean pystyy poistamaan useimmat virukset. Jopa monta kertaa saman ohjelman perään tarttuneet Jerusalem B-virukset saadaan poistettua. Eräät virukset saattavat pilata uhrinsa niin, ettei virusta voida poistaa ohjelmaa vahingoittamatta. Yankee Doodlen poistamisyritys EXE-tiedostosta tuottaa ilmoituksen

```
C:\DOS>CLEAN ATTRIB.EXE [Doodle]
CLEAN 2.1V55 Copyright 1989 by McAfee Associates.
(408) 988-3832
Cleaning [Doodle]
Scanning C:ATTRIB.EXE
  Found Yankee Doodle Virus [Doodle]
  Virus cannot be safely removed from this file.
  Do you want to overwrite and delete "ATTRIB.EXE"
[Y/n]?
```

Tässä tapauksessa Clean suosittelee saastuneen ohjelman poistamista siten, että tiedosto kirjoitetaan ensin täyteen nollaa ja poistetaan vasta sen jälkeen.

Cleanin uudempia versioita on paranneltu niin, että ne pystyvät poistamaan myös Yankee Doodle-viruksen tiedostoa vahingoittamatta.

Ohjelmatiedostoihin tarttuneita viruksia ei yleensä kannata lähteä poistamaan, eikä poisto aina ole edes mahdollista. Jos ohjelmasta on olemassa alkuperäinen levyke tai puhtaaksi tiedetty varmuuskopio, kannattaa mieluummin palauttaa se käyttöön ja tuhota viruksen saastuttama versio. Levykevirusten kohdalla tilanne on toinen; puhdistusohjelman käyttö on joskus ainoa tapa saada levy puhdistettua kohtuuvaivalla.

Tarkistus jokaiseen ohjelmaan

Eräs mahdollisuus virusten torjumiseksi olisi lisätä jokaiseen sovellusohjelmaan osuus, joka aina käynnistyksen yhteydessä tarkistaisi onko ohjelman koodia muutettu ja antaisi tarvittaessa varoituksen käyttäjälle. Näin torjuntaa voitaisiin siirtää loppukäyttäjältä sovellusohjelmien tekijöille.

Tarkistuksessa käytetty ohjelmakoodi tai algoritmi ei kuitenkaan saa olla sama kaikissa ohjelmissa, sillä muuten virukset oppivat kiertämään sitä ja vaikuttamaan tarkistukseen niin, ettei se enää tehoa. Parasta olisi, jos tarkistus olisi erilainen jopa saman ohjelman eri versioissa.

Tällaiset suojausmenetelmät tulevat varmasti yleistymään tulevaisuudessa. Eräissä sovelluksissa asiaa on jo kokeiltukin.

Ellei ohjelmassa ole valmista suojausta, käyttäjä voi lisätä sen itse. F-PROT -paketin mukana tulee F-XLOCK-niminen apuohjelma, joka virusten tapaan kiinnittyy ohjelmatiedoston loppuun ja lisää ohjelman alkuun hypyn itseensä. Kun ohjelma käynnistetään, F-XLOCK tarkistaa sen. Jos ohjelmaan on tullut muutoksia, tulostuu ruudulle ilmoitus "THIS PROGRAM HAS BEEN INFECTED!". Samalla kone pysähtyy.

Tarkistusrutiinin lisääminen ohjelman loppuun kasvattaa sen pituutta 335:llä tavulla. Tarkistusrutiinin voi poistaa F-UNLOCK-ohjelmalla.

Näin on pakko tehdäkin, mikäli ohjelmassa on oma, sisäänrakennettu tarkistus, koska muuten se luulee F-XLOCKia virukseksi.

Muita tarkistavia ohjelmia

Virusvaara on herättänyt myös tavallisten sovellusten tekijät. Tarkistuksia on alettu lisätä sovelluksiin näiden omia toimintoja täydentämään.

Lotuksen Magellan on ohjelma, joka indeksoi levyllä olevat tiedostot. Käyttäjän antamien hakusanojen perusteella löytyy oikea tiedosto muutamassa sekunnissa, vaikka kiintolevyllä olisi tuhansia tiedostoja. Versiossa 2.0 ohjelmaan lisättiin osuus, joka indeksoinnin yhteydessä laskee tarkistussummia ohjelmatiedostoista ja antaa hälyytyksen jos tiedoston sisältö on muuttunut.

HyperAccess/5 keksi ensimmäisenä lisätä tarkistusosuuden tietoliikenneohjelmaan. Kun tiedostoja siirretään ohjelman avulla koneesta toiseen, tarkistetaan samalla niiden sisältö yleisimpien virusten varalta. Ikävä vain, että useimmat tiedostot siirretään nykyisin pakatussa muodossa, jolloin tarkistuksesta ei ole hyötyä.

8

Virustilanne tänään ja huomenna

Virusten torjunta muodostaa sodan, jossa osapuolina ovat virusten ja niiden torjuntaohjelmien tekijät. Aina, kun toinen osapuoli keksii jotain uutta, vastaa toinen siihen samalla mitalla. Viruksista tulee yhä monimutkaisempia ja ne piiloutuvat yhä tehokkaammin. Toisaalta myös torjuntaohjelmat kehittyvät, ollen aina yhden askeleen jäljessä viruksista.

Tällaisen "kilpavarustelun" luonteeseen kuuluu, ettei kumpikaan osapuoli pääse niskan päälle pitkäksi aikaa. Tilanne säilyy horjuvana tasapainona. Emme tule näkemään tappajaviruksia, jotka leviäisivät kautta maailman tiedostoja tuhoten ja tehden torjunta- ja etsintäohjelmat tehottomiksi. Emme tule myöskään näkemään lopullista torjuntaohjelmaa, joka etsisi ja tuhoaisi kaikki nykyiset ja tulevat virukset yhdellä kertaa.

Virusten kanssa on siis opittava elämään. Ne on laskettava yhdeksi tietoturvan uhkaksi siinä missä huonosti koulutetut käyttäjät, perinteiset varkaat ja rikki menevät laitteetkin.

Kirjan kahdessa viimeisessä luvussa tarkastellaan virusten tulevaisuudennäkymiä, pohditaan niihin liittyviä uhkia sekä käsitellään tietoturvaa tavalla, joka ei useinkaan juolahda tavallisen mikronkäyttäjän mieleen.

Virukset: uhka vai ei?

Maaliskuussa 1990 Ph.D., M.D. Peter Tippett, yksi suojausohjelmiin erikoistuneen FoundationWare-yrityksen perustajista ja sen pääjohtaja, piti esityksen, jossa hän maalaili synkin sanoin virusten luomaa uhkaa. Tippettin mukaan tietokoneviruksista aiheutuu seuraavien viiden vuoden aikana 5-10 miljardin dollarin taloudelliset menetykset. Hän perusteli laskelmiaan havaittujen virusten määrällä ja matemaattisilla malleilla, jotka kuvaavat virusten leviämistä mikronkäyttäjien rajoitetussa populaatiossa.

Teoreettiset laskelmat näyttävät vakuuttavilta, mutta ne eivät voi ennustaa, miten moni viruksista aiheuttaa todellista vahinkoa tai sitä, miten tavalliset käyttäjät reagoivat viruksiin. Lisääntynyt puhe viruksista ja torjuntaohjelmien leviäminen nostavat käyttäjien valppautta ja yhä useampi virus saadaan ajoissa kiinni. Tämän osoitti konkreettisesti AIDS-troijalaisen saama maailmanlaajuinen huomio. On silti luonnollista, että torjuntaohjelmien valmistaja haluaa antaa viruksista uhkaavan kuvan.

Luotettavan kuvan saaminen virusten levinneisyydestä on vaikeata. Virus saattaa pilata yrityksessä monta mikroa ilman, että kukaan osaa edes epäillä viruksen olleen asialla. Pilalle menneet tiedostot ja toimimasta lakanneet kiintolevyt menevät helposti vanhojen tuttujen ongelmien piikkiin. Pidetään jopa luonnollisena, että koneet ja niiden tiedostot silloin tällöin lakkaavat toimimasta. Ovathan tietokoneet useimmille käyttäjille kuitenkin salaperäisiä ja kummallisia laitteita, joita ei voikaan täysin ymmärtää.

Koska läheskään kaikki virukset eivät aiheuta varsinaista tuhoa, ne voivat levitä hyvinkin laajalle ennen kuin kukaan edes huomaa mitään poikkeuksellista. Henkilöt, jotka virusten torjunnasta vastaavat, käyttävät yleensä vain virusten etsintään tarkoitettuja ohjelmia. Ne löytävät kyllä vanhat, etsintäohjelman tekijän tiedossa olleet virukset, mutta eivät tiedä mitään uusista viruksista. Tälläkin hetkellä käyttäjien koneissa ympäri maailman liikkuu varmasti useita viruksia, joita kukaan ei ole koskaan huomannut. Osa niistä on saattanut levitä hyvinkin laajalle. Virusten tekijät haluaisivat varmaan jo huutaa maailmalle,

että "Hei, minä tein viruksen! Kertokaa miten sillä menee! Minne asti se on levinnyt?" mutta eivät tietenkään uskalla.

Nekin, jotka ovat viruksen saaneet ja onnistuneet pääsemään siitä eroon, eivät aina ole halukkaita kertomaan havainnoistaan. Virusepidemian löytyminen yrityksestä on huonoa mainosta ja tekee ainakin sen yhteistyökumppanit varovaisiksi. Likapyykki pestään mieluummin yrityksen sisällä. Näin siitä huolimatta, että virus saattaa olla ehtinyt levitä jo talon ulkopuolellekin.

Virusuhkan kehittymistä on vaikeata ennustaa. Varmaa kuitenkin on, että uusia viruksia tulee ilmestymään koko ajan lisää. Virusten tekeminen helpottuu koko ajan, sillä alan tietämys leviää harrastajien keskuudessa nopeasti ja vastuuttomat ohjelmoijat jopa levittelevät virusten lähdekielisiä listauksia. Kreikassa tiedetään alan lehtienkin syyllistyneen viruslistausten julkaisemiseen.

Onko tappajavirus mahdollinen?

Hyvistä yrityksistään huolimatta lääketiede on vieläkin voimaton monien sairauksien edessä. Syöpää ei ole voitettu, vaikka sen tutkimiseen on uhrattu valtavasti aikaa ja rahaa. Jos AIDS olisi keskiaikaisen mustan surman tapaan levinnyt pelkän kosketuksen avulla, olisi koko länsimainen lääketiede suistunut kaaokseen. Oli onnellinen sattuma, että AIDS-viruksen leviäminen rajoittui lähinnä sukupuolisuhteisiin ja likaisiin huumeneuloihin.

Samalla tavalla kohtalokkaita tauteja ei voi kuitenkaan syntyä tietokoneissa. Se, että lääketiede on joutunut tunnustamaan voimattomuutensa, johtuu vain tiedon puutteesta. Emme ihan tarkkaan tiedä, miten ihminen loppujen lopuksi toimii. Kun emme ymmärrä kaikkia mekanismeja, emme voi myöskään puuttua niihin emmekä korjata niissä olevia vikoja.

Tietokoneissa asiat ovat toisin. Koneet ovat ihmisten tekemiä, eikä niiden toiminnassa ole mitään, mitä emme tuntisi tai ymmärtäisi. Kaikki on vain bittien liikettä muistipaikasta toiseen. Tästä syystä kaikki nykyiset ja tulevat tietokonevirukset ovat nujerrettavissa - mutta helppoa se ei tule olemaan.

Etsintäohjelmat paras turva

Helpoin ja tehokkain tapa torjua viruksia on käyttää niiden etsintään tarkoitettuja apuohjelmia. Kuten edellisessä luvussa todettiin, etsintäohjelmat ovat helppoja käyttää ja toimivat varsin luotettavasti. Tavallinen mikronkäyttäjä ei osaa asentaa muistinvaraisia tarkkailuohjelmia eikä jaksa ylläpitää tiedostojen pituuksia tarkkailevaa tietokantaa. Kuka tahansa pystyy kuitenkin tarkistamaan etsintäohjelmalla oman kiintolevynsä ja saamansa levykkeet.

Jotta etsintäohjelmista olisi todellista hyötyä, niitä pitäisi levittää tarpeeksi laajalle. Mikrotukihenkilöiden, mikromyyjien ja alan kerhojen pitäisi jakaa etsintäohjelmia ja näyttää samalla, miten niitä käytetään. Levyjen tarkistaminen virusten varalta pitäisi sujua yhtä automaattisesti ja luonnollisesti kuin varmuuskopion tekeminen. Näin maahan saapuvat virukset voidaan havaita riittävän ajoissa eivätkä ne ehdi levitä laajemmalle.

Vaikka etsintäohjelmat eivät tunnekaan uusimpia viruksia ja vaikka muutamat virukset pystyvätkin huijaamaan niitä, riittää laajamittainen etsintäohjelmien käyttö ehkäisemään isot virusepidemiat. Suurin osa liikkeellä olevista viruksista kun on yleisiä, kauan tunnettuja perusviruksia. Kestää aikansa, ennen kuin maailmalla tehdyt uudet virukset löytävät tiensä Suomeen. Siihen mennessä etsintäohjelmatkin on jo ehditty saattaa ajan tasalle.

Etsintäohjelmien yleistynyt käyttö on selvästi vaikuttanut virusepidemioiden luonteeseen. Isojen, maailmanlaajuisten ongelmien sijasta virustapaukset ovat olleet paikallisia ja pieniä, mutta määrältään sitäkin lukuisampia. Brain-virus levisi aikanaan 300000 levykkeelle, koska viruksista ei puhuttu eivätkä käyttäjät osanneet varautua niihin. Näin suuren epidemian toistuminen on lähes mahdotonta.

Viruksetkin kehittyvät

Kehitys kehittyy, sanotaan. Tässä tapauksessa kehitys koskee niin torjuntaohjelmia kuin viruksiakin. Uusia, entistä tehokkaampia viruk-

sia on jo tekeillä. Ne piiloutuvat entistä tehokkaammin, ohittavat DOSin ja sitä vartioivat apuohjelmat sekä koodaavat itsensä etsintäohjelmien hämäämiseksi. Seuraavassa pari esimerkkiä siitä, mitä tuleman pitää.

1260-virus

Eräs näistä toisen sukupolven viruksista on 1260-virus, joka löydettiin tammikuussa 1990. Se tarttuu COM-tiedostoihin kasvattaen niiden pituutta 1260:llä tavulla. Virus ei jää keskusmuistiin, mutta aina kun saastunut ohjelma käynnistetään, virus etsii levyltä muita COM-tiedostoja ja kopioi itsensä niihin. Koska virus ei jää muistiin, eivät muistinvaraiset torjuntaohjelmat havaitse sitä. Virus ei tartu COMMAND.COMiin.

Viruksen löytämisen tekee vaikeaksi se, että virus koodaa itsensä ohjelman perään. Vanhoista koodaavista viruksista poiketen 1260:n käyttämä koodiavain vaihtelee, eikä kahdessa tartunnan saaneessa COM-ohjelmassa ole kuin muutama yhteinen tavu. Tämä vaikeuttaa etsintäohjelman työtä. Virus ohittaa monissa kohdin DOSin tehden siten useimmat muistinvaraiset torjuntaohjelmat tehottomiksi.

4096-virus

Vuoden 1989 lopulla löydettiin toinenkin vaarallinen virus: 4096. Virus tarttuu sekä COM- että EXE-tiedostoihin ja kasvattaa niiden pituutta nimensä mukaisesti tasan neljällä kilotavulla. Virus tarttuu myös COMMAND.COMiin ja pääsee näin muistiin heti kun kone käynnistetään.

4096-virusta on vaikeata havaita, koska se pystyy mm. vaikuttamaan DIR-käskyn toimintaan. Kun levyn sisältöä katsotaan DIR-käskyllä, virus vähentää saastuneiden ohjelmatiedostojen pituuksista 4096 tavua, jolloin tiedostojen pituus ei näytä muuttuneen. Virus osaa välttää myös useimmat muistinvaraiset tarkkailuohjelmat ja se on itse koodattu.

Virus merkitsee tiedostot, joihin se on jo tarttunut, kasvattamalla niiden päiväystä sadalla vuodella. Koska DIR-listauksessa näkyvät vain vuoden kaksi viimeistä numeroa, ei muutos näy käyttäjälle. Jopa Nortonin levyntutkimisohjelmakin näyttää vuodesta vain kaksi viimeistä numeroa.

Virus on vaarallinen, koska se sotkee kiintolevyn tiedostot linkittämällä niiden FAT-osoittimia ristiin. Linkitys tapahtuu hitaasti ja voi kulua monta viikkoa, ennen kuin käyttäjä huomaa mitä on tekeillä. Lopulta tiedostot ovat niin sekaisin, ettei niitä enää voi käyttää. Ohjelmat saattavat antaa kummallisia virheilmoituksia ja jos kaksi ohjelmaa on linkitetty ristiin, saattaa DOS tulostaa virheilmoituksen "Error in EXE-file" (suomennetussa DOS-versiossa "Virhe EXE-tiedostossa") kun tällaista ohjelmaa yritetään käynnistää.

Jos koneen päiväys on 22. syyskuuta tai tätä myöhäisempi, viruksen saaneet ohjelmat lakkaavat toimimasta. Näyttää siltä, että virus on joko jäänyt tekijältään hieman keskeneräiseksi tai sitten siihen on jäänyt ohjelmointivirheitä. Viruksen koodista voi päätellä, että tekijän tarkoituksena on ollut juhlistaa Taru sormusten herrasta-kirjan Frodoa, jonka syntymäpäivä 22.9. on, kirjoittamalla levyn käynnistyslohkoon teksti "Frodo lives". Nyt tämä osuus ei toimi vaan jumiuttaa koneen.

Viruksen voi havaita epäsuorasti CHKDSK:n avulla, sillä se huomaa ristiin linkitetyt tiedostot ja antaa niistä virheilmoituksia. CHKDSK huomaa myös, ettei DIR-listauksessa lukeva pituus pidä yhtä FATissa varatun tilan kanssa ja antaa virheilmoituksen "Size allocation error" jokaisen viruksen saastuttaman ohjelman kohdalla. Ilmoitusta ei tule, ellei virus ole aktiivisena muistissa, koska silloin ohjelmat näkyvät todellisessa pituudessaan.

Jos virus havaitaan ajoissa, on ohjelmatiedostojen puhdistaminen helppoa. Virus nimittäin poistaa itsensä jokaisesta COPY-käskyllä kopioitavasta tiedostosta. Saastuneiden ohjelmatiedostojen kopiointi levykkeelle tai toiseen hakemistoon kiintolevyllä riittää poistamaan viruksen ohjelmista. Jopa tiedoston kopiointi tyhjään laitteeseen (COPY tiedosto NUL) riittää. Viruksen poistaminen ei kuitenkaan korjaa FATiin tehtyjä virheitä. Myös tiedostoista tehdyt varmuuskopiot saattavat samasta syystä olla käyttökelvottomia.

Virus havaittiin ensi kertaa Suomessa toukokuussa 1990. Se oli päässyt maahan Israelissa tehdyn ohjelman alkuperäisellä levykkeellä. Kaikeksi onneksi valveutunut maahantuoja huomasi koneittensa sekoamisen ja virus paljastui, ennen kuin levykkeitä ehdittiin toimittaa asiakkaille.

4096-viruksesta liikkuu paljon virheellistä tietoa. Eräs dokumentti väittää sen jopa olevan kaikista viruksista vaarallisin ja kertoo, ettei kukaan viruksen saaneista ole toipunut siitä. Tällainen liioittelu ja virheellisten tietojen levittäminen on virusten kohdalla valitettavan yleistä. Kun todellista tietoa ja omakohtaisia kokemuksia viruksesta ei ole, lähtevät huhut helposti liikkeelle.

Syyskuussa 1989 Hollannista löydetty Zero Bug-virus osaa myös piiloutua tehokkaasti. Se tarttuu COM-tiedostoihin kasvattaen niiden pituutta 1536 tavulla, mutta tämäkään lisäys ei näy DIR-listauksessa. Dark Avengerin tapaan virus pyrkii tarttumaan ensin COMMAND. COMiin ja sen jälkeen kaikkiin avattaviin COM-tiedostoihin. Virus on kuitenkin 4096:een verrattuna perin harmiton: kuvaruudulle tulostuu hymyileviä naamoja (PC ASCII-koodi 1), jotka "syövät" kaikki ruudulla näkyvät nollat.

Toukokuussa 1990 eristetty FISH-virus on tehty 4096-viruksen pohjalta, mutta virusta on edelleen kehitetty. Samalla sen koko on pienentynyt 3584 tavuun. Nimensä virus on saanut koodin lopusta löytyvästä merkkijonosta "FISH FI". Kun virus on purkanut itsensä muistiin, se sisältää muidenkin kalojen nimiä (mm. TROUT, COD, TUNA, SHARK).

FISH-virusta on erittäin vaikeata havaita, sillä se on moneen kertaan koodattu. Virus vaihtaa koodausavainta joka päivä ja ollessaan aktiivisena keskusmuistissa se käy säännöllisin väliajoin koodaamassa itsensä uudelleen. Kehittyneisyydestä kertoo myös se, että virus pystyy ohittamaan lähes kaikki muistinvaraiset torjuntaohjelmat.

Virus tarttuu kaikkiin avattaviin tiedostoihin, mutta pituuden lisääntyminen ei näy DIR-komennolla.

Pedon luku

"Pedon luku"-virus on saanut nimensä viruskoodin lopussa olevasta merkistä "666". Monen muun viruksen tapaan tämäkin havaittiin ensiksi Bulgariassa.

Pedon luku on tiedostovirus, joka tarttuu ajettaviin ohjelmatiedostoihin. Virus on vain 512 tavun mittainen, mutta sitä on lähes mahdotonta havaita nerokkaan piiloutumistavan vuoksi. Kun virus tarttuu ohjelmaan, se siirtää 512 ensimmäistä tavua ohjelman loppuun ja kirjoittaa oman koodinsa niiden paikalle. Koska käyttöjärjestelmä varaa tiedostoille tilaa 512, 1024, 2048, 4096 tai 8192 tavun erissä, löytyy lähes jokaisen ohjelmatiedoston lopusta riittävästi tyhjää tilaa virukselle.

Ohjelmat, jotka etsivät viruksia levyltä tai laskevat tiedostoista tarkistussummia eivät pysty havaitsemaan virusta, koska virus antaa pyytävälle ohjelmalle alkuperäiset 512 tavua. Ainoa tapa havaita aktiivisena oleva virus on etsiä sitä suoraan keskusmuistista.

Kaksitoista kujetta

"Twelve tricks trojan (TTT)" eli kahdentoista kujeen troijalainen on esimerkki kehittyneestä ja vaarallisesta Troijan hevosesta. Ohjelma koostuu kahdesta osasta: troijalaisesta, joka istuttaa vahinkoa tekevän osuuden levylle sekä varsinaisesta vahinko-osuudesta. Kyseessä ei ole virus, sillä kumpikaan ohjelma ei pyri tarttumaan toisiin ohjelmiin. Ehkä tekijän ohjelmointitaidot ovat loppuneet kesken ja hän on joutunut tyytymään yksinkertaisempaan troijalaiseen, joka sekin on jo huolestuttavan tehokas.

Kun troijalaisen sisältävää ohjelmaa ajetaan koneessa, se istuttaa vahinkoa tekevän osuuden koneen osiotaulukkoon. Taulukkoon kirjoitetaan lisäksi kopiosuojausten valmistajana tunnetun Softlokin nimi (SOFTLoK+ V3.0 SOFTGUARD SYSTEMS INC) sekä sen osoite ja puhelinnumero. Nimen toinen O-kirjain on jostain syystä kirjoitettu pienellä, vaikka oikean yrityksen nimessä se onkin isolla. Tekijällä on ilmeisesti ollut jotain hampaankolossa Softlokia vastaan.

Koska osiotaulukon kirjoittamisessa ei käytetä DOSin keskeytyksiä, eivät muistissa olevat vartijaohjelmat pysty huomaamaan sitä. Itse troijalainen on lisäksi koodattu niin, etteivät erilaiset tutkimisohjelmat löydä siitä vaaralliselta näyttäviä käyttöjärjestelmäkutsuja tai ohjelman käyttämiä merkkijonoja. Koodi puretaan vasta ajon aikana.

Osiotaulukosta varsinainen vahinko-osuus pääsee muistiin aina kun kone käynnistetään. Se kopioi itsensä (205 tavua) keskusmuistin alussa olevan keskeytysosoitteiden taulukon päälle. Koska viimeisiä keskeytyksiä ei yleensä käytetä, ei ohjelma estä mikron normaalia toimintaa. Koska ohjelma sijaitsee DOSin työalueen ulkopuolella, se ei vähennä käyttäjän näkemää vapaata muistia. Ohjelma ei myöskään käytä mitään DOS-kutsuja, jotka voisivat johtaa sen paljastumiseen.

Muistiin päästyään ohjelma arpoo satunnaisesti yhden kujeen. Kujeita on kaikkiaan kaksitoista ja ne kaikki häiritsevät jollakin tavoin mikron normaalia käyttöä: levyn lukukäskyt muuttuvat kirjoituskäskyiksi, ylimääräinen silmukka hidastaa mikron kaikkia toimintoja, kuvaruudulle syntyy aukkoja, koneen kellonaikaa ei voi asettaa, kello pysähtyy, kirjoittimelle menevä tulostus sekoaa ja niin edelleen. Kaikki katalia temppuja, joiden sattuessa käyttäjä alkaa epäillä koneen olevan rikki ja vie sen huoltoon. Huolto ei löydä koneesta mitään vikaa - ihmettelee vain, miksi salaperäiset oireet näyttävät vaihtuvan aina kun kone sammutetaan ja käynnistetään uudelleen.

Kujeidensa lisäksi ohjelmassa on satunnaislukuarvonta, joka keskimäärin yhdellä kerralla 4096:sta tyhjentää koneen nollauran. Työn jälkeen ruudulle tulostetaan osiotaulukossa oleva SOFTLoK-teksti, jotta yritys saisi syyt niskoilleen. Käyttäjä uskoo, että levy on mennyt rikki Softlokin käyttämän suojauksen vuoksi. Tyhjentämisen vaihtoehtona on FATiin tehtävä muutos, joka kumuloituessaan sekottaa lopulta koko levyn.

Erään teorian mukaan ohjelma, joka istuttaa troijalaisen uuteen ohjelmaan, olisi itsekin troijalainen. Liikkeellä voi siten olla useita troijalaisen saastuttamia ohjelmia ja pahaa-aavistamattomat käyttäjät saattavat jopa itse synnyttää uusia troijalaisia.

Etsivä löytää

Virukset kehittyvät ja oppivat piiloutumaan yhä paremmin ja paremmin. Oikein tehty virus pystyy huijaamaan melkein mitä tahansa etsintäohjelmaa, mutta vain silloin kun se on aktiivisena. Jos kone käynnistetään puhtaalla DOS-levykkeellä, ei virus pysty välttämään ilmituloa. Tästä syystä mitä tahansa virusta vastaan on mahdollista kehittää oma etsintä- ja puhdistusohjelmansa. Ennen kuin ohjelma voidaan kehittää, pitää virus kuitenkin havaita, eristää ja tutkia. Ja se tekee hommasta hankalan.

Hiljaa pahaa tulee

Pahinta, mitä virus voi tehdä, on käyttäjän kiintolevyn tyhjentäminen. Vai onko sittenkään? Jos varmistukset ovat kunnossa, voidaan työtiedostot palauttaa ja mikron käyttöä jatkaa ainakin jollain tavalla jo seuraavana päivänä.

Huomattavasti pelottavampi on jo pelkkä ajatuskin viruksesta tai Troijan hevosesta, joka käy hiljalleen sotkemassa levyllä olevia työtiedostoja. Koska työtä tehdään vaivihkaa, ehtii vahinko levitä pitkälle ennen kuin käyttäjä huomaa mitä on tekeillä. Käyttäjän hyvässä uskossa tekemistä varmuuskopioista ei ole mitään hyötyä. Vaikka tiedostot näyttävätkin päällisin puolin olevan kunnossa, on niiden sisältö pelkkää puppua. Tällaista tuho-ohjelmaa kutsutaan nimellä "hiipivä kuolema" (creeping death).

Työtiedostojen sotkeminen on ikävä kyllä varsin helppoa. Helpointa se on tekstitiedostoilla. Virus voisi vaihtaa kaikki tekstissä esiintyvät a-kirjaimet e-kirjaimiksi, minä-sanat sinä-sanoiksi, lisätä tekstiin ylimääräisiä lauseita FuManchu-viruksen tapaan ja niin edelleen. Tällaisen käsittelyn saanut teksti näyttää nopeasti katsottuna olevan aivan kunnossa. Vasta kun sitä alkaa lukea huomaa, ettei tekstissä ole mitään järkeä.

Ellei tekstitiedostoja sotkeva virus tyytyisi vaihtelemaan pelkästään kirjaimia, olisi se riippuvainen tekijänsä kielestä. Tämä suojelee meitä

suomalaisia mikronkäyttäjiä. Ylimääräiset vieraskieliset sanat erottuvat suomalaisesta tekstistä helposti.

Numerotiedostojen sotkeminen on paljon helpompaa ja kansainvälisempää, joskin vahinkoa rajoittaa eri ohjelmien käyttämät toisistaan poikkeavat tiedostoformaatit. Taulukkolaskentaohjelmista yleisin on Lotus ja sen kanssa rinnakkainen ohjelma Sinfonia. Tämänkin kirjan lukijoista varmaan joka toiselta löytyy koneensa levyltä Lotuksen käyttämiä .WR1, .WK1 tai .WK3-tiedostoja. Vaikka tiedostojen sisältö onkin binaarimuodossa, on Lotus julkistanut tiedostoformaatin kaikkien halukkaiden saataville. Kuka tahansa ohjelmointia tunteva pystyy tekemään Basic-ohjelman, joka lukee ja kirjoittaa Lotuksen käyttämiä työtiedostoja.

Virus voisi etsiä levyllä olevat laskenta-arkit ja muuttaa niissä olevia lukuja tai kaavoja muutamalla prosentilla jompaan kumpaan suuntaan. Tällaisten muutosten vaikutus kumuloituisi mallin summakaavoissa ja saattaisi johtaa käyttäjää pahasti harhaan. Kun ohjelma ilmoittaa, että lopputulos on 5382742 markkaa ja 13 penniä, kukapa sitä uskaltaisi epäillä? Suuretkin taloudelliset päätökset tehdään luottaen sokeasti mikron antamiin lukuihin. Yritys saattaisi ajautua jopa konkurssiin jos sen käyttämät laskentamallit äkkiä menettäisivät arvonsa.

Salakavala virus tai troijalainen (Troijan laiva?) tulee mieleen kun muistelee Wärtsilä meriteollisuuden tapahtumia syksyllä 1989. Oliko taloushallinnon mikroissa virus, joka esti oikeiden lukujen saamisen ja johtopäätösten tekemisen? Vai miten muuten on selitettävissä, ettei yritys nähnyt edessä olevia talousongelmia ennen kuin vasta muutamaa kuukautta ennen konkurssia?

Taulukkolaskennan varassa tehdään muitakin ehdotonta oikeellisuutta vaativia päätöksiä. Esimerkiksi Lotus Sinfonian projektipäällikkö Ray Ozzie kertoi tajunneensa vastuunsa ohjelmoijana vasta, kun eräs sydänkirurgi kertoi käyttävänsä ohjelmaa leikkauksen aikana tietojen analysointiin.

Tekstinkäsittelyn ja taulukkolaskennan lisäksi tarvitaan myös kortisto- ja tietokantaohjelmia. Alan markkinajohtaja on aina ollut dBase. Sen käyttämän .DBF-tiedoston muoto on yksinkertainen ja ylei-

sesti tunnettu. Tietueissa olevien teksti- ja numerokenttien sotkeminen olisi edellä kuvailtujen tapojen yhdistelmä.

Todellisia tiedostoja muuttavia viruksia ei ole vielä löydetty - tai ainakaan kukaan ei ole älynnyt syyttää virusta sattuneista vahingoista.

Tiedostokohtaisia viruksia on kuitenkin jo löydetty. DBF-tiedostoihin erikoistunut dBase-virus ei ole niin kehittynyt, että se muuttaisi kenttien sisältöä, mutta senkin käyttämä tapa on ilkeä: kun dBase kirjoittaa levylle, virus vaihtaa levylle meneviä tavuja keskenään. Lukuvaiheessa virus palauttaa tavut takaisin alkuperäisille paikoilleen, jolloin kaikki näyttää toimivan normaalisti. Tieto siitä, mitkä tiedostot on käsitelty ja mitkä tavut vaihdettu, virus kirjoittaa piilotettuun BUG.DAT-tiedostoon. Se luodaan samaan hakemistoon DBF-tiedostojen kanssa. Kun BUG.DAT-tiedoston päiväys on yli 90 päivää vanha, virus tuhoaa FATit ja päähakemiston kaikilta koneessa olevilta loogisilta levyasemilta.

Jos virus havaitaan ajoissa ja saastunut dBase-ohjelma korvataan uudella, ei viruksen käsittelemiä DBF-kortistoja pystytä enää lukemaan. Samasta syystä myös tiedostoista tehdyt varmuuskopiot ovat käyttökelvottomia.

Virus rakennussarjasta?

Suurin este uusien virusten syntymiselle on siinä, että niiden tekeminen on niin vaikeata. Kokeilun- ja kujeilunhaluisia tekijöitä kyllä riittäisi. Todellinen painajainen pääsisi valloilleen jos joku vastuuton huippuohjelmoija laatisi virusten tekemiseen sopivan työkalun, eräänlaisen virusten rakennussarjan ("Virus construction kit"). Tällaisesta sarjasta voisi kuka tahansa harrastaja rakentaa oman, muista poikkeavan ja siksi hakuohjelmille tuntemattoman viruksen. Muutamassa kuukaudessa erilaiset virukset lisääntyisivät ja täyttäisivät mikrot.

Jo pelkkä ajatuskin rakennussarjasta on pelottava. Onneksi sellainen kääntyisi väistämättä myös tekijöitään vastaan, sillä kukaan mikron käyttäjä ei ole täysin suojassa viruksilta. Viruksia rakentaneen harrastajankin hymy hyytyisi, kun toisten tekemät virukset sotkisivat hänen oman koneensa.

Atari ST-koneille tehty virusten rakennussarja on jo olemassa. Tämä saksalainen neronleimaus on nimeltään VCS (Virus Construction Set) ja se toimii Atarin GEM-käyttöliittymässä. Käyttäjä voi osoittaa valikosta, miten hän haluaa viruksensa leviävän, mihin tiedostoihin tarttuvan ja mitä sen pitää aktivoituessaan tehdä. Sarjan mukana tulee myös ohjelma, jolla tehtyjä viruksia voi jäljittää ja poistaa.

Ultimate parasite

Termillä "Ultimate parasite" (äärimmäinen loinen) kutsutaan ohjelmointikielen kääntäjään lisättyä Troijan hevosta. Kun kääntäjällä tehdään uutta ohjelmaa, kääntäjä lisää sen koodiin jotakin ylimääräistä. Lisäys voi olla looginen pommi, joka esimerkiksi poistaa kaikki levyllä olevat tiedostot 1.1.2000 tai jotain paljon hienompaa, kuten salaovi, josta troijalaisen tekijä pääsee käsiksi ohjelmaan ohittaen kaikki siinä olevat suojaukset. Koska kääntäjää käytetään yleensä myös kääntäjän seuraavan version tekemiseen, leviää myös kaikkiin kääntäjän tuleviin versioihin.

Kääntäjässä oleva Troijan hevonen on erityisen vaarallinen, koska sitä on lähes mahdotonta havaita. Se syntyy automaattisesti jokaiseen käännettävään ohjelmaan. Tällaisen troijalaisen löytyminen isosta ja strategisesti tärkeästä tietokoneesta olisi tuhoisaa, koska troijalaisen tekijä voisi ohittaa kaikki koneeseen ohjelmoidut suojaukset.

Ultimate parasite on mielenkiintoinen ajatusleikki. Huhutaan, että sitä olisi kokeiltu jo käytännössäkin. Huhun mukaan Ken Thompson, eräs Unix-käyttöjärjestelmän alkuperäisistä suunnittelijoista, muutti Unixin mukana toimitettavaa C-kääntäjää niin, että se lisäsi jokaiseen käännettävään Login-ohjelmaan takaoven. Login-ohjelmaa käytetään Unix-koneissa käyttäjän tunnistamiseen ja ennen kuin lupa myönnetään, ohjelma kysyy häneltä käyttäjätunnuksen ja salasanan. Salaoven kautta Ken olisi päässyt sisään mihin tahansa maailman Unix-järjestelmään sen salasanoista ja käyttäjätunnuksista huolimatta. Huhun mukaan joku kuitenkin huomasi salaoven ja se saatiin poistettua.

Kun muistaa, miten Morris käytti hyödykseen Unixin postiohjelmassa vuodesta 1985 asti ollutta takaovea, on tähänkin tarinaan helppo

uskoa. Puolitoista vuotta Internet-madon tapauksen jälkeen asiantuntijat väittivät, ettei madon käyttämiä aukkoja ollut useimmissa Unix-järjestelmissä vieläkään korjattu.

D-aseet

Ihminen on ollut aina hyvä keksimään aseita. Jo historian hämärästä lähtien on aseita tehty tulesta, puusta ja raudasta. Jopa eläimet keksittiin valjastaa sotateollisuuden palvelukseen. Myöhemmin aseiksi alettiin takoa biologiaa, kemikaaleja ja ydinenergiaa. Tätä taustaa vasten on vain luonnollista, että tietokoneetkin lisätään arsenaaliin.

Tietokoneet ovat jo kymmeniä vuosia toimineet sotien taustalla. Sotalaitos ymmärsi tietokoneiden merkityksen jo silloin, kun talouselämä vielä laski palkat käsin, piti kirjanpitoa kynällä ja paperilla eikä uneksinutkaan muusta. Kun ensimmäiset tietokoneet 1940-luvun lopulla rakennettiin, tapahtui kehittelytyö pitkälti armeijan tarpeisiin. Kuvaavaa on, että ensimmäinen työ, mihin nämä monikäyttöiset työkalut laitettiin, oli ammusten lentoratojen laskeminen.

Esi-isiään miljoona kertaa nopeammat tietokoneet laskevat näitä samoja laskuja vielä tänäkin päivänä, mutta esittävät tulokset värillisinä kaavioina ja animaatioina alkuperäisten reikäkorttien sijaan. Lisäksi ne tarkkailevat vihollisen ilmaliikennettä, hoitavat maailmanlaajuista viestiverkostoa ja ajavat sotaa simuloivia ohjelmia. Kolmas maailmansota on käyty tietokoneiden muistissa jo monta kertaa. Oma pieni tietokoneensa löytyy myös ohjuksista, panssarivaunuista ja muista sotakoneista.

Vaikka tietokoneet ovat tähän saakka välttyneet varsinaiselta sotimiselta, saattavat data-aseet olla käytössä jo seuraavan ison konfliktin sattuessa. D-aseet täydentäisivät hyvin nykyisten ABC-aseiden (atomi, biologia, kemia) kirjoa.

Ei siis ihme, että virukset, madot, Troijan hevoset ja loogiset pommit kiinnostavat suuresti armeijan asiantuntijoita. Erityisen aktiivinen on ollut Pentagon, joka on perustanut projektiryhmän tutkimaan virusten käyttöä sodankäynnissä. Tarkoitus on ujuttaa virus vastustajan järjestelmiin joko radioaalloilla tai puhelinlinjoja pitkin. USAn kannal-

ta tilanne on kuitenkin sikäli kiusallinen, että sen todennäköiset vastustajamaat ottavat vasta ensi askelia tietokoneistumisessa. Kaikkein haavoittuvin virussodankäynnissä olisi USA itse.

Turvallisuussyistä NSA (National Security Agency) yritti estää kirjan alussa kerrottuun Internet-matoon liittyvän tietouden leviämisen maan rajojen ulkopuolelle. Kiitos kansainvälisten tietoverkkojen ja elektronisen liikennöinnin helppouden se ei tässä kuitenkaan onnistunut. Samoista syistä yritetään myös estää tietokoneiden toimittaminen itä-Eurooppaan, vaikka kauppasaarron alkuperäiset syyt ovat jo aikaa sitten poistuneet.

NSA on estänyt myös yleisesti tunnetun DES-salausalgoritmin tai sitä käyttävien ohjelmien viemisen ulkomaille. USAssa myydään monia aivan tavallisia sovellusohjelmia (kuten PC-Tools tai Superkey), jotka käyttävät tätä algoritmia tiedostojen salakirjoittamiseen. Koska tällaisia ohjelmia ei saa myydä eikä viedä ulkomaille, on niistä tehty erityiset vientiversiot, joista salausalgoritmi on joko kokonaan poistettu tai se on korvattu vähemmän tehokkaalla. Liikkuu myös huhuja, joiden mukaan NSA olisi lisännyt algoritmeihin salaisia parametreja. Nämä parametrit tuntemalla NSA voisi itse helposti purkaa muiden DESillä salaamat viestit.

Tietokoneet tekee houkuttelevaksi maaliksi niiden keskeinen asema tämän päivän elämässä. Samalla, kun yhteiskunta on siirtänyt tietojaan ATK-aikaan, se on myös tullut suoraan riippuvaiseksi tietoja käsittelevistä koneistaan. Voi vain kuvitella, millainen kaaos syntyisi, jos virus tai jokin muu tuhoaisi pankkien tilitiedot, poliisin rikosrekisterin, valtion väestökirjanpidon tai verottajan tiedostot. Jo pelkkä sähkökatko riittää pysäyttämään koko normaalin elämänmenon. Kansalaiset eivät edes heräisi aamuisin, ellei heidän kelloradionsa soisi.

Isoa virusepidemiaa ei suotta kutsuta "ydinpommin taloudelliseksi vastineeksi".

Virus kilpailuaseena

Sotaa käydään myös armeijan ulkopuolella. Tämän sodan kohteena ovat markkinaosuudet ja sitä käydään joka päivä. Taistelijoina ovat

liike-elämän palveluksessa olevat naiset ja miehet, aseina mainoskampanjat, hinnoittelu, tuotepolitiikka ja myyntiennusteet. Voittoja lasketaan kaatuneiden sijasta pörssikursseina ja tilinpäätöksinä. Ja taistelut ovat kovia.

Mitä tapahtuisi, jos keskenään kilpailevat suuret ohjelmatalot laittaisivat liikkeelle toistensa ohjelmia tuhoavia viruksia? Tai jos ne onnistuisivat istuttamaan viruksen kilpailijansa alkuperäisille ohjelmalevykkeille? Jo pelkkä tieto siitä, että jostain ohjelmasta on löydetty viruksia, riittäisi pelottamaan monet sen käyttäjistä eikä ohjelmaa ostettaisi.

Viruksen ei välttämättä tarvitsisi tuhota mitään. Sellainen paljastuisi nopeasti ja saattaisi kääntyä tekijäänsä vastaan, jos asia pääsisi julkisuuteen. Paljon tehokkaampaa olisi tehdä virus, joka tuottaisi kohteeseensa epämääräisiä vikoja ja saisi sen toimimaan epäluotettavasti. Kun sana ohjelman epäluotettavasta toiminnasta leviäisi, laskisi myös sen myynti.

Epäreiluja keinoja on itse asiassa jo käytetty, vaikkakin hieman toisella tavalla. Kopiointisuojausten tekemiseen erikoistunut Vault Corporation kertoi julkisesti valmistaneensa suojausmenetelmän, joka sotkisi käyttäjän kiintolevyn, mikäli suojausta yritettäisiin murtaa. Ilmoitus aiheutti niin suurta vastarintaa käyttäjissä, etteivät sovellusten tekijät uskaltaneet ottaa Vaultin kopiosuojausta käyttöön. Silti ilmoituksella oli psykologinen merkitys: nyt suojauksia murtavat käyttäjät joutuvat pelkäämään tätäkin mahdollisuutta.

Toinen tapaus liittyy tiedostoon SUG.ARC, joka lupasi poistaa kopiosuojauksen levykkeiltä, joiden suojaukseen oli käytetty Softguardin ohjelmaa. Käynnistyksen jälkeen SUG.COM pyysi käyttäjää laittamaan alkuperäisen ohjelmalevykkeen A: asemaan ja tulosti tämän jälkeen ruudulle tekstin:

```
You have violated the license agreement under which you received
the software. All of your data has been destroyed. This
destruction constitutes prima facia evidence of your criminal
violation. If you attempt to challenge Softguard Systems, Inc. or
the software vendor in court, you will be vigorously counter-sued
for infringement and theft of services; we believe that our case
will have more merit to it than yours.  If you have any questions
concerning this matter, you are invited to contact our lawyers at
the following address:
```

```
Softguard Systems Incorporated
```

Teksti kertoi ohjelman tuhonneen käyttäjän tiedostot kostoksi siitä, että käyttäjä oli yrittänyt murtaa Softguardin kehittämän suojauksen ja näin rikkoa ostohetkellä tekemäänsä ohjelman käyttösopimusta vastaan.

Epäselväksi jäi, oliko tuho-ohjelman tekijä todella Softguard Systems vai oliko joku (kenties kilpaileva Vault) halunnut mustata Softguardin mainetta.

Keväällä 1990 tuli Japanissa ilmi tapaus, jossa nimeltä mainitsematon tietokonealan yritys oli palkannut opiskelijoita kehittämään viruksia, jotka oli suunnattu kilpailevia Sharp-tietokoneita vastaan.

9

Mikrot ja tietoturva

Tietotekniikassa alkoi 1980-puolivälissä rakennemuutos, joka tulee vaikuttamaan rajusti koko alan kehitykseen. Muutoksen moottorina ovat mikrotietokoneet. Varsinkin lähiverkkoihin asennettuna ne ovat alkaneet syrjäyttää perinteisiä keskuskoneeseen ja päätteisiin pohjautuvia tietojärjestelmiä.

Mikroilla onkin monia etuja. Ne ovat keskenään yhteensopivia, jolloin valmistajien välinen kilpailu pitää hinnat alhaisina. Ohjelmavalikoima on valtava, eikä mikron käyttäjä ole sidottu laitevalmistajan tarjoamiin ohjelmiin. Tuhannet ja taas tuhannet insinöörit työskentelevät mikrojen parissa, mikä takaa nopean laite- ja ohjelmateknisen kehityksen. Syntyy hypertekstin ja julkaisuohjelmien kaltaisia uusia sovellusalueita. Ja niin edelleen. Ei ihme, että mikrot ovat vallanneet yritykset ja isojakin sovelluksia on siirretty keskuskoneista mikroverkkoihin.

Jotain on kuitenkin unohtunut.

Keskuskoneaikaan operaattorit valvoivat koneen käyttöä. He hoitivat varmuuskopioinnin ja tiedostojen suojaamisen. Koska tietokonetta käytettiin yksinkertaisilta päätteiltä, tallentuivat kaikki tiedostot keskustietokoneen uumeniin. Tietokonekeskukseen pääsivät vain tarkoin valitut henkilöt, mikä teki fyysisen tietovarkauden vaikeaksi.

Nyt samoja sovelluksia ollaan siirtämässä mikroverkkoihin. Tärkeät tiedostot sijaitsevat palveluasemassa, joka on vain yksi mikro muiden joukossa. Ovi huoneeseen, jossa palveluasema on, ei useinkaan ole edes lukossa. Satunnainen ohikulkija tekee hetkessä kiintolevyn tiedostoista ylimääräiset "varmuuskopiot" levykkeille, pistää ne taskuunsa ja kävelee ulos kenenkään huomaamatta.

Tavallista mikroa on hyvin vaikeata suojata niin, että tiedostojen kopiointi levykkeille estyisi. Näppäimistön voi lukita ja hakemistoja jakaa salasanoja käyttäen, mutta tällaiset niksit on mahdollista kiertää. Jos ei muu auta, voi koneesta katkaista hetkeksi sähköt ja käynnistää sen tavallisella DOS-levykkeellä A: asemasta. Kun DOS on ladattu, voi kiintolevyä käyttää mielin määrin. Verkon kaatuminen havahduttaa tietenkin käyttäjät, mutta ennen kuin kukaan heistä ehtii palveluaseman luo tutkimaan asiaa, on tekijä jo kaukana.

Asiattoman käytön estämiseksi on eräisiin mikroihin lisätty numerokoodi, joka kysytään ennen kuin alkulataus käynnistetään. Ellei koodia tunne, ei käynnistyskään onnistu. Käynnistyskoodi tallennetaan CMOS-RAMiin, jonka voi tyhjentää avaamalla koneen ja irrottamalla akkuun tai paristoon menevän johdon. Suojaus ei siten ole täysin luotettava.

Työasemassa tietosuojan toteuttaminen on helpompaa. Käytettävissä ovat vain ne hakemistot, jotka palveluaseman hoitaja on jakanut yleistä käyttöä varten. Nämäkin hakemistot voidaan suojata niin, ettei hakemistoon pysty itse kirjoittamaan mitään. Eräissä verkoissa voidaan jopa tiedostojen kopiointi työasemaan haluttaessa estää.

Verkkojen yleistymisen myötä markkinoille ovat tulleet erityisesti verkon työasemiksi suunnitellut pikkumikrot. Niissä on vain keskusyksikkö, näyttölaite, näppäimistö ja verkkokortti. Levykeasemaa tai kiintolevyä ei ole lainkaan. Jopa koneen käynnistäminen ja käyttöjärjestelmän lataaminen tapahtuu verkon läpi. Näin voidaan olla varmoja siitä, ettei käyttäjä kopioi verkossa olevia tiedostoja omille levykkeilleen eikä toisaalta kopioi palveluasemaan viruksen saastuttamia ohjelmia.

Kaikista keksinnöistä huolimatta mikrot säilyvät aina henkilökohtaisina tietokoneina. Tietoturvan toteuttaminen niissä on vaikeata. Kun mikroja kehitettiin, suunnittelijoiden mielessä oli tietojen jakaminen eikä niiden salaaminen.

Lähiverkko sinänsä on kiitollinen vakoilun ja tarkkailun kohde, sillä siinä kulkevaa tietoliikennettä on erittäin helppo seurata. Ethernet-verkossa voidaan mistä tahansa työasemasta sopivan ohjelman avulla nähdä koko verkossa kulkeva liikenne.

Verkon käyttöön liittyy paljon arkisempiakin riskejä. Hyvä esimerkki näistä on osaston yhteiskäytössä oleva laserkirjoitin. Yleensä

se kytketään palveluasemaan, jolloin verkon käyttäjät voivat omalta työasemaltaan lähettää sille tulostuksia. Mitään luottamuksellisia töitä ei kuitenkaan kannata tulostaa, sillä ne lojuvat laserissa kuin tarjottimella ja ovat kaikkien ohikulkijoiden nähtävissä. Pahimmassa tapauksessa käyttäjä ei muista, montako tulostusta hän on verkkoon lähettänyt, jolloin ylimääräiset paperit saattavat lojua laserilla päiväkausia. Palveluaseman tulostusjono saattaa olla jumissa tai tulostaa tekstit useana kopiona, mikä riittää sekoittamaan tulostajan omat laskelmat.

Lähiverkkojen lisäksi mikrojen tietoturvaa uhkaavat monet muutkin tekijät.

Tietoliikenneohjelmien salasanat

Sielläkin, missä isot keskuskoneet yhä puolustavat linnaketta, ovat mikrot päässeet jo uloimmille suojavarustuksille asti korvaamalla vanhat tietokonepäätteet. Yhteys keskuskoneeseen voidaan luoda suorana linjayhteytenä, lähiverkon kautta tai puhelimen ja modeemin avulla.

Mikron tietoliikenneohjelma hoitaa merkkien lähettämisen keskuskoneelle ja sen antamien vastausten lukemisen. Ohjelmiin on tehty monia käyttömukavuutta parantavia ominaisuuksia. Esimerkiksi sisäänkirjoittautuminen (login) eli käyttäjätunnuksen ja salasanan antaminen on mahdollista automatisoida ns. skriptejä käyttämällä. Nämä skriptit suorittavat toistuvat rutiinitehtävät käsin koskematta.

Skriptit tallennetaan mikrossa levylle omina ohjelminaan. Kun ne ovat levyllä, voi kuka tahansa lukea skript-ohjelman sisällön TYPE-käskyllä ja nähdä käyttäjän tunnuksen ja salasanan. Jotta näin ei kävisi, ei salasanaa pitäisi kirjoittaa valmiiksi skriptiin, vaan se pitäisi syöttää näppäimistöltä jokaisen sisäänkirjoittautumisen aikana.

Virus tositarkoituksella

Tässä kirjassa on moneen otteeseen neuvottu, miten tavallinen mikronkäyttäjä voi pienentää virustartunnan riskiä. Kokonaan mainitsematta

on jäänyt se mahdollisuus, että joku voisi levittää viruksia aivan tarkoituksella.

Mikä olisikaan tehokkaampi tapa tuottaa harmia työtoverilleen kuin antaa hänelle "lahjaksi" viruksen saastuttama peliohjelma? Lahja olisi varminta antaa juuri kun saaja tai antaja on itse lähdössä talosta, ikään kuin läksiäislahjana. Näin vastuuton antaja voisi itse välttää saamasta sitä.

Entä sitten mikrotukihenkilö, joka lähtee talosta ovet paukkuen? Jos hän viimeisenä työpäivänään levittää viruksen lähiverkon palvelukoneeseen ohittaen kaikki siihen ja käyttäjien työasemiin rakentamansa virussuojat, ehtii virus aiheuttaa melkoiset vahingot ennen kuin seuraava tukihenkilö ehtii korjata tilanteen.

Aina löytyy vastuuttomia tai vihansa sokaisemia henkilöitä, jotka ovat valmiita tuottamaan harmia muille. Koska joku saattaa levittää viruksia aivan tarkoituksella, ei kiinni saatuja viruksia pidä koskaan jakaa toisille käyttäjille, ei edes "tutkimustarkoituksiin", vaikka nämä sitä pyytäisivätkin.

Pahinta näissä tarkoituksella levitetyissä viruksissa on se, ettei tekijää useinkaan saada kiinni. Ja vaikka saataisiinkin, on häntä hyvin vaikeata saada vastuuseen teostaan. On lähes mahdotonta todistaa, keneltä virus on päässyt verkkoon ja että teko on ollut tahallinen. Onhan virus voinut levitä aivan vahingossakin. Syyllinen voi aina väittää, ettei ole tiennyt ohjelmassa olleesta viruksesta.

ATK-lainsäädäntö on kaikissa maissa laahannut pahasti suorien ja epäsuorien tietokonerikosten jäljessä. USAssa välimatkaa on pyritty kuromaan umpeen lakeja tiukentamalla, sillä jo vuonna 1986 hyväksyttiin tietokoneiden väärinkäytön ja tietokonekavallukset tuomitseva laki.

Esimerkiksi Donald Burleson, joka potkut saatuaan asensi työpaikan koneeseen 168000 myyntipalkkiotietoa tuhonneen madon, sai seitsemän vuoden ehdollisen vankeustuomion ja 11800 dollarin sakot. Internet madon tehnyt Morris pääsi nuoruutensa ja kokemattomuutensa vuoksi vähemmällä.

Myös Länsi-Saksassa tunnetaan laki tietokonesabotaasista. Raskain tuomio voi olla viisi vuotta vankeutta.

Mikro yhteiskäytössä

Tietoturvan kannalta heikoimpia ovat mikrot, joilla on monta käyttäjää. Takavuosina tällaiset ratkaisut olivat jopa yleisiä, koska mikrot olivat kalliita. Nyt yhteismikrot ovat käyneet harvinaisiksi, sillä aleneva hintakehitys on tuonut oman mikron lähes jokaiselle käyttäjälle. Hinta ei muutenkaan näytä olevan este mikron hankkimiselle, sillä eräisiin yrityksiin on hankittu tehokkaita 386-koneita joita sitten käytetään pääte-emulaattorilla.

Tässä kirjassa on jo monta kertaa todettu, että DEL-käskyllä poistetun tiedoston palauttaminen on mahdollista. Jos työpaikan koneella kirjoittaa hakemuksen uutta työpaikkaa varten tai tunteellisen rakkauskirjeen muulle kuin omalle puolisolle, ei pelkkä tiedoston poistaminen riitä takaamaan turvallisuutta. Työpäivän päätyttyä utelias työkaveri, esimies tai mikrotukihenkilö saattaa tulla penkomaan tiedostoja ja palauttaa nekin, jotka käyttäjä on kuvitellut tuhonneensa. Poistetut tiedostot saattavat tulla näkyviin myös aivan vahingossa, kun tukihenkilö yrittää korjata levyyn tullutta vikaa tai palauttaa jotain toista poistettua tiedostoa.

Miten sitten poistaminen pitäisi tehdä, jotta kukaan ei pystyisi palauttamaan tiedostoa? Varminta on jo tekovaiheessa ohjata kaikki luottamukselliset tiedostot levykkeelle, joka sitten työn päättyessä arkistoidaan varmaan paikkaan. Tämäkään tapa ei ole ongelmaton. Jos tiedostot ovat pitkiä, saattaa niiden käsittely levykkeillä venyä kiusallisen pitkäksi ja koneen tehokkuus tuntuu menevän hukkaan. Lisäksi ainakin eräillä tekstinkäsittelyohjelmilla on tapana tehdä käytön aikana tilapäisiä työtiedostoja kiintolevylle, vaikkei työn alla olevaa tiedostoa tallennettaisi mihinkään. Näitä aputiedostoja tutkimalla voi palauttaa ainakin osan tekstistä.

On olemassa apuohjelmia, jotka poistavat tiedostot kiintolevyltä kirjoittamalla niiden päälle nollaa. Tämä takaa, ettei tiedostoa voida palauttaa. Tunnetuin pyyhkimisohjelma on Nortonin mukana tuleva WIPEFILE. Komento

```
C:\TEKSTIT>WIPEFILE RAKKAANI.TXT
```

kirjoittaa RAKKAANI.TXT-tiedoston päälle nollaa ja poistaa sen tämän jälkeen levyn kirjanpidosta. Jos halutaan tyhjentää kokonainen levyke, voidaan käyttää saman paketin WIPEDISK-ohjelmaa. Vuodesta 1990 lähtien myös Mace Utilities-pakettiin sisältyy tiedostoja tuhoava DESTROY-ohjelma.

Ellei sopivaa apuohjelmaa satu olemaan ulottuvilla, voi aina käyttää omatekoista komentojonoa. Alunperin Kiintolevyn käyttäjän oppaassa esitelty PYYHI.BAT-komentojono täyttää kiintolevyllä vapaiksi merkityt alueet ja takaa, ettei tiedostojen palauttaminen onnistu. Komentojono käyttää apuna tiedostoa TAYTE.TXT, joka saa sisältää mitä tahansa tekstiä. Yksikin kirjain (esimerkiksi X) riittää. Tiedoston on kuitenkin oltava puhdasta ASCII:ta, jotta COPY-komento pystyy liittämään kaksi sellaista peräkkäin.

Komentojono PYYHI.BAT näyttää seuraavalta:

```
ECHO OFF
ECHO Odota, täytän kiintolevyn tyhjän tilan...
COPY TAYTE.TXT APU.TXT
:ALKU
COPY APU.TXT+APU.TXT APU2.TXT
DEL APU.TXT
IF NOT EXIST APU2.TXT GOTO TAYNNA
REN APU2.TXT APU.TXT
GOTO ALKU
:TAYNNA
ECHO Käsittely valmis. Poistettuja
ECHO tiedostoja ei voi palauttaa.
```

Komentojono pysähtyy kun tiedosto APU2.TXT on kasvanut niin isoksi, ettei se enää mahdu levylle. Sitä ennen komentojono on kirjoittanut kaikki levyllä vapaiksi merkityt alueet täyteen APU.TXT-tiedostoa eikä alle jääneitä poistettuja tiedostoja voi enää mitenkään palauttaa.

PYYHI.BAT-komentojono on yksinkertainen ja tehokas. Sen ainoana heikkoutena on hitaus. Ison, paljon vapaata tilaa sisältävän kiintolevyn käsittely saattaa kestää useita minuutteja.

Kuka huoltaa koneesi?

Kun mikro jonain kauniina päivänä lakkaa toimimasta, on se toimitettava huoltoon. Monasti asiakas joutuu itse raahaamaan laitteensa huollon vastaanottotiskille. Vain harvoin huolto lähettää jonkun noutamaan konetta. Itse korjaus tapahtuu harvoin asiakkaan luona, vaikka nykyiset moduulirakenteiset mikrot mahdollistaisivatkin sen.

Mikron joutuminen huoltoon on suuri turvallisuusriski. Koneen mukana kannetaan pois kymmenien miljoonien merkkien verran tietoa, joka voi olla korvaamattoman tärkeätä yrityksen toiminnan kannalta tai tuhoisaa kilpailijan käsiin joutuessaan. Kukaan ei antaisi viedä tällaista tietomäärää perinteisissä mapeissa!

Kun huolto sitten tutkii mikroa, se pääsee esteettä näkemään kaikki levyllä olevat tiedot. Huoltohenkilöt voivat myös kopioida levyllä olevat ohjelmat tai tiedostot itselleen. Pahinta on, jos kiintolevy on mennyt rikki. Koska kiintolevyjä ei voida korjata muualla kuin valmistajan tehtaassa, vaihtaa suomalainen huolto rikki menneen levyn uuteen. Käyttäjä ei saa koskaan tietää, mihin hänen levynsä ja tietonsa lopulta päätyvät.

Valveutunut käyttäjä tiedostaa asian, mutta ei välttämättä voi tehdä sille mitään. Jos mikro on niin rikki, ettei se edes käynnisty tai jos vika on kiintolevyllä, ei luottamuksellisia tiedostoja voi poistaa vaikka haluaisikin. Eikä pelkkä tiedoston poistaminen edes riittäisi, sillä jokainen asiansa osaava huoltomies tai mikrotukihenkilö pystyy palauttamaan ne Nortonin kaltaisilla apuohjelmilla. Ainoa tapa suojata tietoja tällaisten tilanteiden varalta on tallentaa tiedostot salasanalla suojattuna, jos käytetty sovellusohjelma siihen pystyy.

Tarkistitko muuten, kuka mikron noutaja todella oli? Esittikö hän korttinsa tai todistiko hän henkilöllisyytensä? Luovutitko kalliin tietokoneen ja arvokkaat tiedot tuntemattomalle miehelle? Jos hän haki poissa olevan naapurisi koneen, oletko varma että mikro edes oli rikki?

Valppauteen olisi syytä, sillä kukapa osaisi epäillä huoltomiestä? Mikron omistaja on vain kiitollinen, kun huolto vihdoin tulee paikalle, eikä välitä asiasta sen enempää.

Uskon, että minäkin voisin kävellä sisään lähes mihin tahansa yritykseen ja kertoa vahtimestarille olevani mikroa noutava huoltomies. Voisin etsiä käsiini haluamani mikron tai tyytyä ensimmäiseen, joka tulee vastaan. Helpointa olisi napata kone tyhjästä huoneesta, mutta vaikka koneen käyttäjä olisi paikallakin, voisi mikron silti napata. Käyttäjälle voisi esimerkiksi kertoa, että kone pitää viedä vuosihuoltoon. Pari sanaa liikkeellä olevasta viruksesta riittäisi myös pelottamaan käyttäjän niin, että hän luopuisi koneestaan ja antaisi sen "puhdistettavaksi".

Eräät suuret yritykset, joiden mikroissa säilytetään poikkeuksellisen tärkeitä tietoja, ovat ottaneet tietoturvan vakavasti. Huollolta on vaadittu takeet siitä, ettei kiintolevyjä lähetetä eteenpäin muualle korjattaviksi. On myös vaadittu, että huolto ei vie koskaan konetta mukanaan, vaan että kaikki korjaukset suoritetaan paikan päällä asiakkaan omissa tiloissa.

Lopuksi pieni vinkki kaikille mikroja huoltaville liikkeille: tarkistakaa huollon päätteeksi myös kiintolevyn puhtaus. Jonkin hyvän virusten etsintäohjelman ajaminen kiintolevyllä ei kauaa kestä. Merkintä "virustarkastus tehty" joko työselosteessa tai koneen kylkeen liimatussa tarrassa ilahduttaa kummasti koneen omistajaa, kun hän saa koneensa takaisin. Hyvä palvelu on pienistä kiinni.

Liite 1

Viruksen tunnistaminen

Kun koneessa havaitaan virus, on ensimmäinen tehtävä yrittää sen tunnistamista. On turha lähteä tyhjentämään koko kiintolevyä, jos virus on niin yksinkertaista tyyppiä, että pelkkä saastuneiden tiedostojen poistaminenkin riittäisi. Virus on helpointa tunnistaa jonkin etsintäohjelman avulla, mutta ellei sellaista ole käytettävissä tai ellei ohjelma tunne koneessa pesivää virusta, voidaan tunnistusta yrittää epäsuorasti.

Tässä liitteessä on esitelty tapoja, joilla viruksen tunnistamista voi yrittää. Näitä ovat mm.

- viruksen aiheuttamat oireet
- määrä, jolla tartunnan saaneet tiedostot pitenevät
- keskusmuistin määrässä tapahtuvat muutokset

Viruksen tunnistaminen oireiden perusteella

On mahdotonta listata kaikkia niitä oireita, joita virukset saattavat aiheuttaa. Oireet ovat usein vielä epämääräisiä, jolloin niitä on vaikea paikallistaa. Seuraavaan listaan on koottu Suomesta löytyneiden virusten aiheuttamia selkeitä oireita, joista voi olla apua viruksen tunnistamisessa.

Kone tekee alkulatauksen (boot) kun ohjelmaa yritetään käynnistää

- Wieniläisvirus

Kuvaruudulle tulostuu teksti "Leagalise marijuana!" kun kone käynnistetään:

- Stoned

Kuvaruudulla näkyy pallo, joka pomppii näytön reunasta toiseen:

- Italialainen

Koneesta kuuluu musiikkia kesken ohjelman käytön:

- Yankee doodle

Kuvaruudulle tulostuu musta alue:

- Jerusalem

Koneen kaiutin piippaa kun ohjelma käynnistetään:

- Vacsina

Näytöllä olevat merkit putoavat ruudun alareunaan:

- 1701/1704

Käynnistettävä tiedosto poistuu:

- Jerusalem

Ohjelma ei enää mahdu muistiin:

- Jerusalem, tartuttuaan monta kertaa EXE-tiedostoon

Koneen toiminta hidastuu selvästi:

- Jerusalem, oltuaan 30 minuuttia muistissa

Ruudulle tulostuu teksti "Disk Killer" ja kiintolevyn valo palaa pitkän aikaa:

- Disk Killer

Ohjelmatiedostojen piteneminen

Ohjelmatiedostoihin tarttuvat virukset kasvattavat väistämättä tidostojen pituutta. Kehittyneimmät virukset pystyvät tosin peittämään jälkensä niin hyvin, ettei pituuden lisääntyminen näy DIR-listauksessa eikä asiaa kysyvällä ohjelmallakaan, jos virus on parasta aikaa aktiivisena muistissa.

Jotta pituuden lisääntyminen voitaisiin mitata, voidaan menetellä esimerkiksi seuraavasti: levylle perustetaan testihakemisto, johon kopioidaan *kirjoitussuojatulta* levykkeeltä uusi ohjelmatiedosto. Tiedoston pituus kirjoitetaan muistiin. Ohjelma ajetaan ja pituutta verrataan tämän jälkeen alkuperäiseen lukemaan. Ellei pituus näytä muuttuvan, käynnistetään kone puhtaaksi tiedetyltä ja kirjoitussuojatulta DOS-levykkeeltä ja tarkistetaan asia uudelleen. Näin voidaan estää muistissa olevaa virusta vaikuttamasta pituuden näkymiseen.

Muutamat virukset selviävät CTRL-ALT-DEL käynnistyksestä, koska se ei tyhjennä RAM-muistia. Tämän estämiseksi on kone aina sammutettava virtakytkintä käyttäen.

Seuraavassa listassa on lueteltu pituus, jolla tiedostovirukset kasvattavat ohjelmaa tarttuessaan siihen. Lopullinen pituuden kasvu saattaa vaihdella hieman ohjelmassa olevista konekielikäskyistä riippuen. Koska viruksista saattaa myös olla liikkeellä hieman toisistaan poikkeavia versioita, tulee listan antamia numerotietoja pitää vain suuntaa-antavina. Viruksen nimen jälkeen on eritelty vielä, onko kyse EXE- vai COM-tiedoston muuttumisesta.

Pituuden lisäys	Virus
163	163-virus
512	Friday 13 COM, COM
534	Toothless, COM
642	Islantilainen, EXE
648	Vienna, COM
656-671	Islantilainen, EXE
669-684	Lauantai 14 päivä, COM ja EXE
847	847-virus, COM
848-863	Islantilainen, EXE
867	Fumble, COM
879	Pretoria, COM
941	Devil's Dance, COM (monta kertaa)
1168	Datacrime 2, COM (ei COMMAND.COM)
1206-1218	Vacsina, COM
1277	Murphy, COM ja EXE
1280	Datacrime, COM (ei COMMAND.COM)
1332	Sylvia, COM (ei COMMAND.COM)
1346-1350	Vacsina, EXE (kahdessa vaiheessa)
1539	XA1, COM
1554-1569	Ten bytes
1560	Alabama
1618-1634	MIX (Islantilainen), EXE
1701-1704	1701/1704, COM
1800	Dark Avenger, COM ja EXE
1808	Jerusalem B, EXE (monta kertaa)
1813	Jerusalem B, COM
1864	dBase-virus, COM ja OVL
1917	Datacrime IIB, COM ja EXE
2080	FuManchu, COM
2086	FuManchu, EXE
2351	Ghost, COM
2756-2806	Oropax, COM (ei COMMAND.COM)
2881-2897	Yankee Doodle, COM ja EXE
2930-3031	Traceback II, COM ja EXE

3066	Traceback, COM ja EXE
3551-3555	SysLock, COM ja EXE
3584	FISH, COM ja EXE
3880	Itavir, EXE
4096	4096-virus, COM ja EXE
5120	VBasic, COM ja EXE

Vapaan muistin väheneminen

Viruksen, joka haluaa säilyä keskusmuistissa, on pakko varata osa muistista itselleen. Muistin väheneminen näkyy CHKDSK:n ilmoittaman alemman muistimäärän laskuna. Ongelmana on se, ettei käyttäjä useinkaan tiedä, paljonko vapaata muistia on ollut ennen tartunnan saamista, ellei tätä lukua ole kirjoitettu ajoissa muistiin.

Seuraavassa taulukossa on lueteltu määriä, joilla eräät Suomesta löytyneet virukset vähentävät vapaana olevan keskusmuistin määrää.

Tavua	Virus
1216	Vacsina
1808	Jerusalem B
3008	Yankee Doodle
3696	Dark Avenger
3824	1701/1704
4096	Stoned
5648	4096
7168	Brain
8384	Disk Killer

Osa viruksista majoittuu vapaan muistin yläpäähän jolloin CHKDSK:n ilmoittama ylempi muistimäärä (=kokonaismuisti) vähenee. Listan lukemat on mitattu koneesta, jossa oli täysi 640 kilon (655360 tavua) muisti.

CHKDSK:n ilmoittama kokonaismuisti	Virus
647168	Disk Killer
648192	Brain
649712	4096
651264	Stoned
651664	Dark Avenger
652352	Yankee doodle
653312	Korealainen

Mikäli koneessa on laajennettu BIOS, saattaa kokonaismuistin vähentyminen aiheutua siitä. Saman vaikutuksen tuottavat mm. eräät lähiverkkokortit. Oleellista kuitenkin on, ettei muistin määrän pitäisi muuttua käytön aikana suuntaan eikä toiseen.

Liite 2

Ohjelmien maahantuojia

Norton Utilities, Proscan, Turbo Anti-Virus:
Holosoft, puh. (941) 871 201

Manifest, Mace Utilities, Vaccine, PC-Tools, Certus:
MikroMartti, puh. (90) 692 3800

Manifest, Magellan:
Tietoväylä, puh. (941) 783 344

Check-it!:
Toptronics, puh. (921) 546 666

IBM Virscan:
Kaikki IBM-jälleenmyyjät

McAfeen ohjelmia, FPROT-pakettia ja lukuisia muita PD- ja shareware-ohjelmia kannattaa kysellä toisilta mikroharrastajilta tai laite- ja ohjelmamyyjiltä. Niitä löytyy myös lähes kaikista hyvinvarustetuista purkeista, joihin voi ottaa yhteyden modeemilla.

Hakemisto

Hakemistossa virusten nimet on merkitty kursiivilla.